АПИНО

ICAIT

10TH INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2021

X ЮБИЛЕЙНАЯ МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ «АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ В НАУКЕ И ОБРАЗОВАНИИ»

СБОРНИК НАУЧНЫХ СТАТЕЙ

24–25 ФЕВРАЛЯ 2021 ГОДА

APINO.SPBGUT.RU

СПбГУТ))) Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

ГОД НАУКИ И ТЕХНОЛОГИЙ В СПбГУТ

АПИНО

ICAIT

10TH INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2021

X ЮБИЛЕЙНАЯ МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ «АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ В НАУКЕ И ОБРАЗОВАНИИ»

Научные направления:

– Радиотехнологии в связи
– Инфокоммуникационные сети и системы
– Информационные системы и технологии
– Теоретические основы радиоэлектроники
– Цифровая экономика и управление в связи
– Гуманитарные проблемы информационного пространства
– Сети связи специального назначения

Партнёры:

Технологии бесконечности
КОМПАНИЯ «Т8»

ООО «Т8»

АРГУС НТЦ

ООО «НТЦ АРГУС»

SERTEK

ООО «Сертек»

Информационные партнёры:

ТУЗС

журнал
«Труды учебных заведений связи»

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ ИНФОРМАЦИЯ КОСМОС

журнал
«Информация и космос»

Информационная поддержка:

www.infocom.sut.ru

электронный журнал «Информационные технологии и телекоммуникации»

24–25 ФЕВРАЛЯ 2021

Санкт-Петербург, пр. Большевиков, 22/1,
Английский пр. 3, наб. р. Мойки, 65

APINO.SPBGUT.RU

УДК 001:061.3(082)
ББК 72 А43

Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С. В. Бачевского; сост. А. Г. Владыко, Е. А. Аникевич.
СПб. : СПбГУТ, 2021. Т. 2. 623 с.

В научных статьях участников конференции исследуются состояние и перспективы развития мирового и отечественного уровня IT и телекоммуникаций. Предлагаются методы и модели совершенствования научно-методического обеспечения отрасли связи и массовых коммуникаций.

Предназначено научным работникам, аспирантам и студентам старших курсов телекоммуникационных и политехнических вузов, инженерно-техническому персоналу и специалистам отрасли связи.

Научное издание
Литературное редактирование,
корректура Е. А. Аникевич
Оформление Г. И. Юрьев
Верстка Е. М. Аникевич
Подписано в печать 02.08.2021.
Вышло в свет 31.08.2021. Формат 60×90 1/8.
Уст. печ. л. 77,875. Заказ № 073-ИТТ-2021.
пр. Большевиков, д. 22, корп. 1.
Россия, Санкт-Петербург, 193232

ISBN 978-5-89160-231-1

СОДЕРЖАНИЕ

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

УДК 004.9
ГРНТИ 20.15.13

ИНФОРМАТИЗАЦИЯ ТАЙМ-МЕНЕДЖМЕНТА ПРИ АВТОМАТИЗАЦИИ ДОРОЖНЫХ ЦИФРОВЫХ ТАБЛО

А. В. Авнигина, А. В. Фёдорова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье дается понятие о дорожных цифровых табло переменной информации, о способах их крепления и дополнительных элементах. Сравниваются табло переменной информации с динамическим информационным табло по техническим характеристикам. Обосновывается необходимость применения тайм-менеджмента. Предлагаются способы его информатизации при процессе автоматизации дорожных цифровых табло.

тайм-менеджмент, управление, время, дорожное табло, дорожные знаки, табло переменной информации, дорожные сенсоры, информационные системы.

Проблема модернизации автомобильных дорог всегда являлась актуальной для России [1]. Для повышения пропускной способности и увеличения безопасности дорог необходима техническая поддержка, а также новые подходы к управлению дорожным движением [2].

Дорожное цифровое табло – это табло, закрепляемое на специальной опоре, которую устанавливают на трассах с 3-мя и более полосами. Табло состоит из нескольких модулей – для информации о дороге и дорожных знаках, обычно это знаки ограничения скорости. Пример такого табло показан на рис. 1. В данном случае оно предназначено для 4-х полос, движущихся в одну сторону.

Рис. 1. Дорожное цифровое табло переменной информации.
Источник: Оборудование для АСУДД и систем весового контроля. Ссылка: https://profinzhenerstroj.tiu.ru/p291205922-oborudovanie-dlya-asudd.html

Также на этой опоре могут установить метеостанцию, дорожные сенсоры, сенсоры трафика и камеры. Метеостанция включает в себя атмосферные датчики и дорожные сенсоры.

Рассматриваемые пример относится к классу «Табло переменной информации» (ТПИ). Также существует еще один вид табло, называемый «Динамические информационные табло» (ДИТ). ДИТ – это трехстрочное информационное табло с графическим полем, которое находится слева или справа от текстового поля. Оно предназначено для вывода буквенно-цифровой информации и графического изображения [3]. Пример такого табло показан на рис. 2.

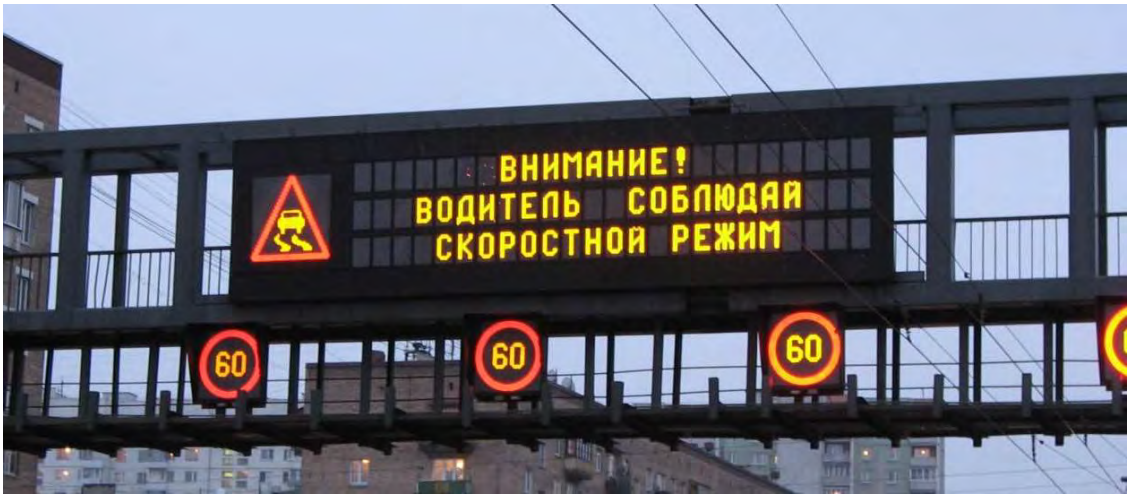


Рис. 2. Динамическое информационное табло.
Источник: Динамическое информационно табло. Ссылка: http://amonier.by/content/production/informacionnie_tablo/dinamicheskoe_informacionnoe_tablo/

В таблице показано сравнение технических характеристик табло переменной информации и динамическое информационное табло [4, 5].

ТАБЛИЦА. Сравнение технических характеристик ТПИ ТБ-511 и ДИТ ЕМР 20С-672160

Сравниваемый параметр	Табло переменной информации ТБ-511	Динамическое информационное табло ЕМР 20С-672160	
Производитель	ООО «Треком»	ООО «Бюро интеллектуальных систем», СПб.	
Габариты табло, мм	Ш×В×Г = = 6 645×1 500×240	Ш×В×Г = 6 840×1 720×200	
Отображаемая информация	Текст и пиктограмма	Текст и пиктограмма	
Тип источника света	DIP-светодиоды	SMD-светодиоды со специализированной фокусирующей линзой	
Производитель светодиода	Неизвестно	NICHIA, Япония	
Формат текстового поля	3 строки по 20 знаков (монохром)	Полная матрица 6 720*1 600 мм Полноцветная	
Высота текстового знака	200 мм		
Размер поля пиктограмм	1 100×1 100 мм		
Структура знака	7×5 пикселей, по 2 светодиода в пикселе	Матрица 336×80 полноцветных диода R+G+B	
Структура поля пиктограммы	48×48 пикселей, по 2 светодиода в пикселе		
Цвет свечения светодиодов знака	Желтый	Полноцветный (RGB)	
Цвет свечения светодиодов пиктограммы	Желтый и красный		
Максимальная яркость	Не менее 9 000 Cd/м^2	Яркость, кд/м^2, не менее / класс по ГОСТ Р 56350-2015:	
		Красный	3 100 / L3
		Зеленый	3 720 / L3
		Синий	1 240 / L3
		Белый	12 400 / L3
		Желтый	7 440 / L3
Число градаций яркости	3	32	
Контрастность	Не менее 7	Класс R2 по ГОСТ Р 56350-2015 (зависит от освещенности, цвета, угла)	
Угол обзора	Не менее 15 градусов	Класс B5 по ГОСТ Р 56350-2015 (0.. ± 15 по горизонтали, 0.. – 5 по вертикали)	
Обслуживание табло	С задней стороны	С задней стороны	
Интерфейс	RS-485	RS-485 и Ethernet 10 TX	

Сравниваемый параметр	Табло переменной информации ТБ-511	Динамическое информационное табло ЕМР 20С-672160
Контроль работоспособности	До блока замены и каждого светодиода	До блока замены и каждого светодиода
Электропитание	Однофазная сеть переменного тока напряжением 220 В (+10 %, –15 %), частотой 50 Гц	Однофазная 220 В или трехфазная 220/380 В сеть (+15–13 %), частотой (50 ± 1) Гц
Потребляемая мощность	Не более 800 Вт	Максимальная мощность (белое поле на максимальной яркости 12 400 кд/м^2) – 2,7 кВт – в момент включения или при проведении тестов. Рабочая мощность (один дорожный знак + три строчки текста на максимальной яркости) ~ 0,7 кВт
Масса табло, кг	Не более 450	Не более 650
Условия эксплуатации	Температура окружающего воздуха от –30 до +50°С, относительная влажность воздуха – до 100 %, атмосферное давление – 630–800 мм рт. ст.	ДИТ предназначено для эксплуатации на открытом воздухе с установленными значениями температуры окружающего воздуха от минус 40°С до плюс 60°С (класс Т1+Т3 по ГОСТ 32865-2014) и относительной влажности 95 % в условиях атмосферного давления от 84 до 106,7 кПа (от 630 до 800 мм рт. ст.). Конструкция изделия обеспечивает стойкость к воздействию соляного тумана в соответствии с требованиями ГОСТ 32865-2014
Класс защиты	IP65	Фронтальная поверхность – IP65 по ГОСТ 14254-2015

Под автоматизацией дорожных цифровых табло поднимется комплекс мер по управлению автоматизацией функционирования этого оборудования [5].

После выполнения сравнительного анализа технических характеристик двух видов дорожных цифровых табло для проведения эксперимента по информатизации функций тайм-менеджмента в предметной области автоматизации цифровых табло были выбраны динамические информационные табло. Так как для автоматизирования дорожных цифровых табло, метеостанций и другого оборудования необходимо затратить много ресурсов – времени, людей, техники, предложено использовать основы управления временем.

Основы управления временем (тайм менеджмент) – это набор методов и методик, реализованных в практических тренингах, помогающих индивидууме или организации эффективно использовать свое время. Эти способы позволяют распоряжаться временам так, чтобы достигать максимальной производительности и высоких личных результатов [6].

Поскольку данными функциями занимается отдел автоматизации, и он работает с информационными системами, было решено использовать информационные системы и технологии при информатизации тайм-менеджмента. Для этого можно использовать как готовые цифровые решения, так и разработать локальное программное обеспечение, ориентированное под решение узкопрофессиональных задач. Это могут быть системы или программы, которые будут управлять процессом изготовления этих табло с точки зрения именно тайм-менеджмента, но в данной предметной области. Например, можно разработать программу для компьютера или телефона, в которой будут собраны все основные операции, порядок их выполнения и время, которое нужно потратить на них. И будут определенные функции напоминания или контроля временного процесса. Поскольку в нашей стране не ведутся разработки в данном направлении, эта область исследования и практического применения является актуальной и востребованной.

Список используемых источников

1. Коноплянко В. И. Организация и безопасность дорожного движения. М. : Транспорт, 1991. 183 с.

2. Косолапов А. В. Повышение эффективности информационного обеспечения участников дорожного движения в городах: дис. …канд. техн. наук : 05.22.10 / Косолапов Андрей Валентинович. М., 1992. 178 с.

3. Светодиодные табло и знаки для организации дорожного движения. URL: http://www.svetoform.ru/znaki-dlya_dorogi.html (дата обращения 27.03.2021).

4. Кременец Ю. А., Печерский М. П., Афанасьев М. Б. Технические средства организации дорожного движения. М.: Академкнига, 2005. 279 с.

5. Жанказиев С. В. Интеллектуальные транспортные системы. М. : МАДИ, 2016. 120 с.

6. Аллен Д. Как привести дела в порядок. Искусство продуктивности без стресса: пер. с англ. В. Каденко. 7-е изд. М. : Манн, Иванов и Фербер, 2014. 268 с.: ил.

УДК 004.056
ГРНТИ 81.93.29

ОЦЕНКА ЭФФЕКТИВНОСТИ ДИАГНОСТИРОВАНИЯ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

В. С. Авраменко, А. В. Маликов

Военная академия связи

В статье рассматривается подход к оценке эффективности диагностирования компьютерных инцидентов в инфокоммуникационных системах. Представлены показатели эффективности, порядок их оценивания. Основное внимание уделено оценке эффективности систем диагностирования компьютерных инцидентов, использующих искусственные нейронные сети.

компьютерный инцидент, эффективность, показатель, оценка, искусственные нейронные сети.

В настоящее время активно развиваются методы и средства управления компьютерными инцидентами (КИ) в инфокоммуникационных системах (ИКС). Одной из ключевых задач управления компьютерными инцидентами является диагностирование КИ – анализ информации состояния ИКС с целью определения значений существенных для принятия решения на реагирование характеристик обнаруженных нарушений безопасности [1, 2].

Оценка эффективности системы защиты информации в ИКС, в том числе и системы диагностирования КИ, является неотъемлемой частью работ по организации защиты как при создании системы, так и в ходе ее функционирования. Оценке эффективности защиты информации в ИКС различного назначения [3, 4], наряду с моделированием защиты информации [5, 6], уделяется достаточно много внимания, но вопросы оценки эффективности диагностирования КИ полностью не исследованы.

Под эффективностью системы диагностирования КИ понимается комплексное операционное свойство процесса функционирования системы диагностирования КИ, характеризующее его приспособленность к достижению основной цели – достоверному определению значений характеристик нарушений безопасности информации в пределах допустимых затрат времени и ресурсов.

В соответствии с одним из принятых в теории эффективности подходов показатель исхода операции по диагностированию КИ представляет собой

вектор, элементы которого отражают результативность (эффект), оперативность и ресурсоемкость диагностирования:

$$Y^{д}_{эф} = < Y^{д}_{э}, Y^{д}_{о}, Y^{д}_{р} > . \quad (1)$$

Результативность диагностирования обуславливается целевым эффектом, ради которого функционирует система диагностирования – достоверное определение значений характеристик нарушений безопасности, обусловившего КИ. Ресурсоемкость характеризуется ресурсами, используемыми для получения целевого эффекта. Оперативность определяется расходом времени, необходимого для диагностирования.

Для оценки эффективности диагностирования целесообразно использовать критерий пригодности. В вероятностной операции диагностирования оцениваемой системе (варианту) диагностирования ставится в соответствие множество исходов операции с известными условными вероятностями появления. Критерий пригодности для оценки эффективности диагностирования:

$$K^{д}_{приг} : P_{дц}(Y^{д}_{эф}) \geq P_{дцтр}(Y^{д}_{эф}) \quad (2)$$

определяет правило, по которому диагностирование считается эффективным в том случае, если вероятность достижения цели по частным показателям эффективности диагностирования $P_{дц}(Y^{д}_{эф})$ не меньше требуемой вероятности достижения цели по этим показателям $P_{дцтр}(Y^{д}_{эф})$.

Под достоверностью диагностирования компьютерного инцидента понимается свойство результатов диагностирования соответствовать фактическим значениям характеристик нарушения безопасности со степенью приближения, позволяющей использовать результаты диагностирования для принятия адекватного решения на реагирование. В общем случае процесс диагностирования является случайным, поэтому в качестве показателя достоверности диагностирования компьютерного инцидента при условии независимости результатов диагностирования от длительности функционирования ИКС может использоваться вероятность правильного диагностирования $P_{прд}$ или вероятность ошибочного диагностирования $P_{ошд}$, которые связаны следующим образом:

$$P_{прд} = 1 - P_{ошд} . \quad (3)$$

Выражение для статистической оценки вероятности правильного диагностирования имеет следующий вид:

$$\hat{P}_{\text{прд}} = \frac{N_{\text{пр}}}{N_{\text{общ}}}, \quad (4)$$

где $N_{\text{пр}}$ – количество правильно определенных значений характеристик в ходе диагностирования, $N_{\text{общ}}$ – общее количество диагностических проверок.

Под оперативностью диагностирования компьютерного инцидента понимается свойство системы диагностирования определять значения характеристик нарушения безопасности за допустимое время. Показателем оперативности диагностирования компьютерного инцидента является вероятность того, что продолжительность диагностирования $t_{\text{д}}$ не превысит допустимое значение $t_{\text{ддоп}}$, то есть $P(t_{\text{д}} \le t_{\text{ддоп}})$.

Ресурсоемкость диагностирования компьютерного инцидента представляет собой свойство системы диагностирования, характеризующее затрачиваемые на диагностирование ресурсы вычислительной системы, такие как процессорное время, оперативная и долговременная память. Также могут быть использованы стоимостные показатели.

Показателем ресурсоемкости является вероятность того, что коэффициент использования ресурсов $K_{\text{р}}^{\text{дг}}$ не превысит допустимое значение: $P(K_{\text{р}}^{\text{дг}} \le K_{\text{рдоп}}^{\text{дг}})$.

Коэффициент использования ресурсов определяется следующим образом:

$$K_{\text{р}}^{\text{дг}} = \frac{C_{\text{дг}}}{C_{\text{о}}},$$

где $C_{\text{дг}}$ – количество ресурсов, затраченных на диагностирование; $C_{\text{о}}$ – общее количество ресурсов.

Частные критерии результативности, оперативности и ресурсоемкости диагностирования могут задаваться следующим образом:

$$P_{\text{прд}} \ge P_{\text{прдтр}},$$

$$P(t_{\text{д}} \le t_{\text{ддоп}}) \ge P_{\text{тр}}(t_{\text{д}} \le t_{\text{ддоп}}),$$

$$P(K_{\text{р}}^{\text{дг}} \le K_{\text{рдоп}}^{\text{дг}}) \ge P_{\text{тр}}(K_{\text{р}}^{\text{дг}} \le K_{\text{рдоп}}^{\text{дг}}),$$

где $P_{\text{прдтр}}$ – требуемое значение вероятности правильного диагностирования.

Векторный показатель (1) позволяет более полно оценивать исходы операции по диагностированию, чем скалярный. Но часто на практике из-за сложности задачи нахождения оптимальных решений по векторному пока-

зателю прибегают к скаляризации путем аддитивной или мультипликативной свертки частных показателей в один обобщенный. При наличии доминирующего показателя допустимо использовать способ выделения главного показателя, остальные либо отбрасываются, либо для них устанавливаются допустимые значения. В качестве доминирующего показателя эффективности диагностирования КИ целесообразно использовать показатель достоверности, так как именно степень соответствия результатов диагностирования реальным значениям характеристик нарушений безопасности в основном определяет уровень адекватности реагирования.

В рамках реализации перспективного подхода к диагностированию компьютерных инцидентов для реализации классификатора применяются искусственные нейронные сети, в частности – многослойный персептрон [2, 7]. Соответственно, достоверность диагностирования КИ в таких системах определяется общепринятыми показателями качества нейронных сетей: точность (*accuracy*), *A*, полнота (*recall*), *R*, специфичность (*specificity*), *S*.

Точность указывает на долю правильных ответов из общего числа ответов классификатора.

Полнота показывает долю правильных ответов классификатора из общего числа примеров одного класса.

Специфичность, как и полнота, показывает долю правильных ответов классификатора из общего числа примеров, но только для противоположного класса.

На рис. 1 изображено наглядное представление показателей полноты *R* и специфичности *S*.

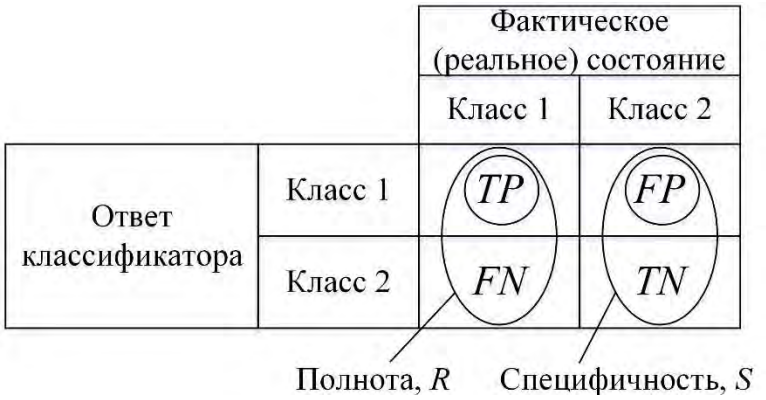


Рис. 1. Составляющие показателей полноты *R* и точности *S*

Формулы для вычисления значения показателей точности, полноты и специфичности имеют вид:

$$A = \frac{TP + TN}{N_{\text{общ}}}; \tag{5}$$

$$R = \frac{TP}{TP + FN}; \quad (6)$$

$$S = \frac{TN}{TN + FP}. \quad (7)$$

Показатель точности согласно формуле (5) фактически соответствует показателю достоверности согласно формуле (4). При этом в ходе тестирования должны использоваться выборки одинакового объема. На практике не всегда удается получить выборки одинакового объема для разных характеристик нарушения безопасности. В этом случае предпочтительно использовать показатели полноты и специфичности согласно формулам (6) и (7).

Значение показателя полноты и специфичности стремятся максимизировать за счет построения оптимальной структуры многослойного персептрона и обучения его на репрезентативном наборе обучающих примеров.

Таким образом, для оценки эффективности системы диагностирования целесообразно использовать векторный показатель эффективности (1) и критерий пригодности (2). Также может использоваться способ выделения главного показателя, в качестве которого выступает показатель достоверности (3). Но для подходов к диагностированию с применением методов машинного обучения целесообразно использовать показатели полноты (*recall*) и специфичности (*specificity*), так как они характеризуют достоверность результатов определения каждого значения искомой характеристики нарушения безопасности.

Список используемых источников

1. Авраменко В. С. Модели защищенности информации от несанкционированного доступа в многорежимных автоматизированных системах и методы ее контроля в условиях неопределенности угроз // Информация и космос. 2008. № 2. С. 87–94.

2. Авраменко В. С., Маликов А. В. Диагностирование нарушений безопасности информации в инфокоммуникационных системах на основе искусственных нейронных сетей // Региональная информатика и информационная безопасность : сб. тр. конф. Вып. 4. СПб.: СПОИСУ, 2017. С. 24–26.

3. Паращук И. Б. Показатели качества системы обеспечения безопасности информационных технологий в управлении и оценивание эффективности ее функционирования // Информационные технологии в управлении (ИТУ-2018) : материалы конф. 2018. С. 389–393.

4. Саенко И. Б., Лаута О. С. Оценка киберустойчивости компьютерных сетей на основе результатов стохастического моделирования компьютерных атак // Информационные технологии в управлении (ИТУ-2016). Материалы 9-й конференции по проблемам управления. Председатель президиума мультиконференции В. Г. Пешехонов. 2016. С. 768–773.

5. Лепешкин О. М., Маслов О. Н., Худайназаров Ю. К. Моделирование процесса управления безопасностью системы связи // Инновационная деятельность в Вооруженных Силах Российской Федерации : тр. всеармейской науч.-прак. конф. 2017. С. 212–214.

6. Буйневич М. В., Емельянов А. А. Модель функционирования системы защиты от НСД к критическим информационным ресурсам при проектировании АСУ // Автоматизация процессов управления. 2009. № 3. С. 97–104.

7. Авраменко В. С., Маликов А. В. Методика диагностирования компьютерных инцидентов безопасности в автоматизированных системах специального назначения // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 1. С. 44–52.

УДК 004.032.26, 004.896
ГРНТИ 28.23.37, 50.51.15

ПАРАМЕТРИЧЕСКАЯ ОПТИМИЗАЦИЯ СЛОЖНОГО ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ВЫТЯГИВАНИЯ ОПТИЧЕСКОГО ВОЛОКНА

А. М. Адуевский, К. В. Кучеревский, М. Ю. Савин, Д. В. Соловьев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящей статье рассматривается метод параметрической оптимизации технологического процесса вытягивания оптического волокна из заготовки с помощью технологий искусственных нейронных сетей.

системы автоматизации проектирования (САПР), искусственные нейронные сети, оптическое волокно, многослойный персептрон, алгоритм обратного распространения ошибки.

Современное общество находится на этапе внедрения компьютерной техники и искусственного интеллекта во все области производства. Так же в ближайшее время прогнозируется массовое внедрение так называемых киберфизических систем во все отрасли промышленности [1]. Наиболее важной задачей в разработке системы автоматизации проектирования (САПР) является разработка качественно новых методов автоматизации проектирования, а наиболее важной задачей при автоматизации проектирования является разработка математического обеспечения САПР технологического процесса (ТП). Целью автоматизации проектирования математического обеспечения является снижение затрат на рабочую силу, получение большего количества готовой продукции при сохранении качества, экономия ресурсов и т. д. Выделяют следующие этапы проектирования математического обеспечения САПР ТП: этап идентификации технологического процесса, этап синтеза систем управления технологического процесса, этап оптимизации проектных, управляющих решений, этап прогнозирования

параметров технологического процесса. Рассмотрим особенности проектирования математического обеспечения на последних двух этапах для технологических процессов оптического производства, в частности для технологического процесса изготовления оптических волокон. Технологический процесс вытягивания оптического волокна из заготовки является сложным и многостадийным процессом и характеризуется малой информативностью, сложностью физико-химический процессов, нестационарностью и распределенностью сложно контролируемых параметров [2]. Схема установки для вытягивания оптического волокна из заготовки показана на рис. 1.

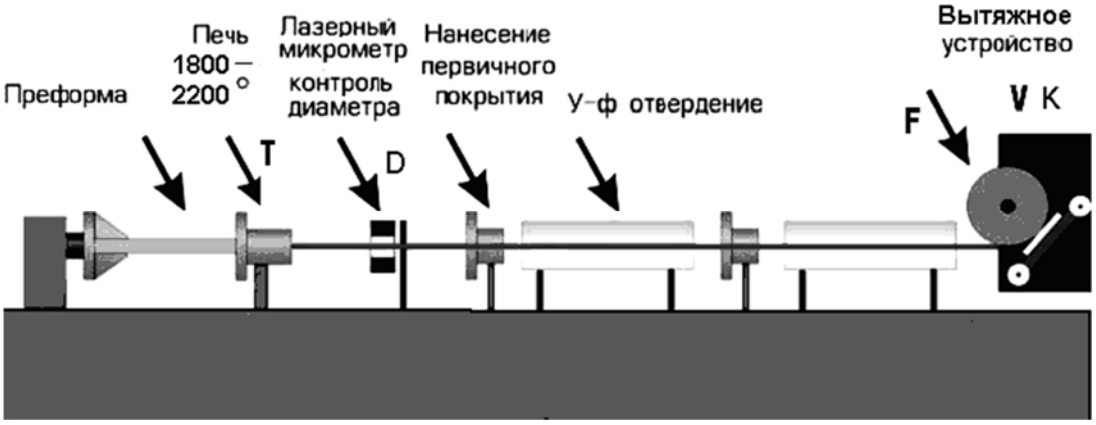


Рис. 1. Схема установки для вытягивания оптического волокна из заготовки

Как правило, так называемая «башня» для получения оптического волокна из заготовки состоит из блока для фиксации и равномерной подачи заготовки в печь, блока для регулирования диаметра извлеченного волокна и блока для нанесения защитных покрытий, ультрафиолетовых ламп для полимеризации акрилата, намоточной машины и шкафов управления для согласования работы всех блоков. Эти устройства могут также включать в себя системы метрологического исследования готового волокна, такие как устройства для определения прочности на «разрыв», устройства для измерения оптических потерь и так далее. Как показывает практика, параметрическая оптимизация этого технологического процесса на лету является чрезвычайно дорогостоящим мероприятием, которое может привести к дальнейшим потерям времени и ресурсов из-за внезапного неконтролируемого увеличения количества брака продукции и необходимости постоянного переналаживания промышленного оборудования. Параметрическая оптимизация может выполняться в виртуальном пространстве компьютера, что позволяет сэкономить дорогое сырье и время на переналадку промышленного оборудования.

В настоящее время для автоматизации проектирования математического обеспечения САПР активно используется нейросетевой подход [3, 4].

Для нейросетевого метода совершенно не имеет значение сущность технологического процесса, который он моделирует, технологический процесс представляется для него «черным ящиком», с необходимостью выполнения условий непротиворечивости и репрезентативности данных в обучающих выборках и наличия функциональных зависимостей между выходными и входными параметрами. В результате чего нейросеть может моделировать любой реально существующий физико-химический процесс. Нами были определены следующие параметры технологического процесса вытягивания оптического волокна из заготовки. Входными параметрами являются температура печи (*T*), диаметр вытягиваемого волокна (*D*), сила натяжения намоточной машины (*F*). Выходными параметрами являются скорость вытяжки (*V*) и комплексный параметр качества волокна (*K*), который рассчитывается исходя из величины оптических потерь готового волокна и количества структурных дефектов в волокне. Для решения задачи параметрической оптимизации технологического процесса была предложена следующая структура нейронной сети (рис. 2).

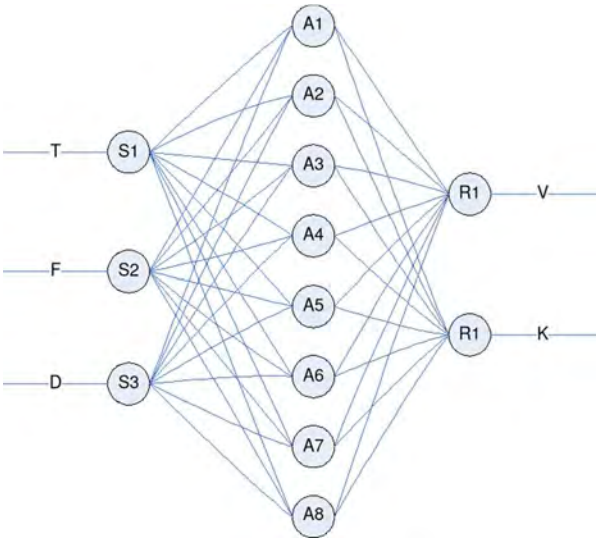


Рис. 2. Структура нейронной сети

В качестве структуры искусственных нейронных сетей (ИНС) был выбран трехслойный персептрон с одним скрытым слоем. Количество входных нейронов равно количеству входных параметров технологического процесса (температура печи – *T*, сила натяжения волокна – *F*, диаметр волокна – *D*). Количество выходных нейронов равно количеству выходных параметров техпроцесса (скорость вытягивания – *V*, критерий качества – *K*). В ходе экспериментов в скрытом слое решено было выбрать 8 нейронов, так как это оказалось оптимальным с точки зрения получения качественного решения за приемлемое время. Входные для ИНС данные нормировались в интервал [0:1], что обусловлено выбором активационной функции нейронов скрытого слоя – гиперболического тангенса.

На выходе так же применялась линейная функция активации. В качестве алгоритма обучения был выбран модифицированный алгоритм обратного распространения ошибки (*Backpropagation*). Классический алгоритм обратного распространения ошибки был модифицирован за счет применения метода градиентного спуска в процессе корректировки весовых коэффициентов и применения так называемых «эпох обучения». Данные для

формирования обучающей выборки фиксировались и записывались в режиме реального времени в лаборатории волоконной оптики в процессе вытягивания оптического волокна диаметром 125 мкм.

Итогом работы предложенного нейросетевого алгоритма параметрической оптимизации стали следующие результаты (рис. 3).

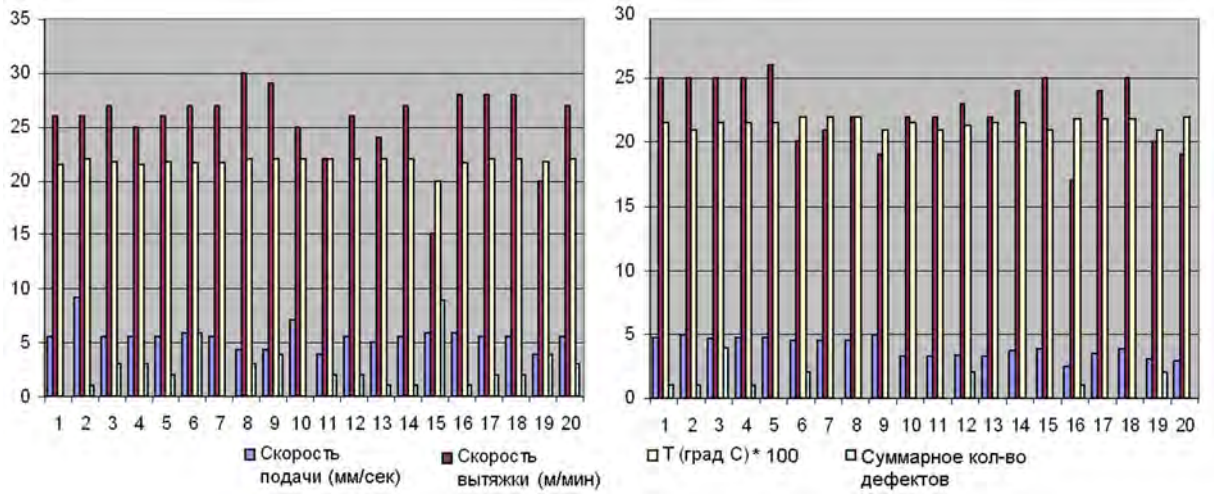


Рис. 3. Слева – график, построенный по данным из обучающей выборки и справа – график, построенный на основе данных искусственной нейронной сети

Анализируя полученные результаты, можно заключить, что ошибка ИНС составила менее 1 %, что говорит о целесообразности применения аппарата ИНС для решения задачи параметрической оптимизации и прогнозирования параметров технологического процесса вытягивания оптического волокна из заготовки. Следует отдельно отметить, что данные, полученные с помощью ИНС, удовлетворяют накладываемым технологическим ограничениям на параметры технологического процесса вытягивания волокна. В виду вышеизложенного можно с уверенностью сказать, что технологии искусственных нейронных сетей – мощный инструмент для автоматизации проектирования математического обеспечения САПР сложных технологический процессов оптического производства.

Список используемых источников

1. Потрясаев С. А. Математическое и программное обеспечение синтеза технологий и планов работы киберфизических систем // Изв. вузов. Приборостроение. 2018. Т. 61, № 11. С. 939–946.

2. Гатчин Ю. А., Бондаренко И. Б., Дукельский К. В. Технология изготовления специальных типов оптических волокон. СПб.: Изд-во политехнического ун-т. 2015. 155 с. ISBN 978-5-7422-5130-9.

3. Соловьев Д. В. Нейросетевой метод оптимизации математических моделей сложных технологических процессов // Научно-технический вестник СПбГУ ИТМО. 2008. № 51. С. 33–39.

4. Соловьев Д. В., Бондаренко И. Б. Параметрическая оптимизация сложных технологических процессов оптического производства с использованием технологий искусственных нейронных сетей // Научно-технический вестник СПбГУ ИТМО. 2010. № 6. С. 70.

УДК 004.056
ГРНТИ 81.93.29

ИСКУССТВЕННЫЕ НЕЙРОННЫЕ СЕТИ В ВОПРОСАХ ОБНАРУЖЕНИЯ НИЗКОИНТЕНСИВНЫХ АТАК НА ОТКАЗ В ОБСЛУЖИВАНИИ НА ИНФОРМАЦИОННУЮ СИСТЕМУ

А. М. Адуевский, К. В. Кучеревский, М. Ю. Савин, Д. В. Соловьев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассмотрены современные сетевые угрозы и атаки DoS и DDoS. Самые распространенной сетевой угрозой на данный момент является DDoS-атака низкой интенсивности. Для обнаружения этих атак используют системы безопасности с использованием искусственных нейронных сетей (ИНС). Данный метод является наиболее эффективным, поскольку ИНС способны обучаться в процессе работы в режиме реального времени.

обнаружение атак, DoS-атака, DDoS-атака, низкоинтенсивная DDoS-атака, искусственная нейронная сеть.

Самой распространенной сетевой угрозой является атака на доступность информации или ресурсов автоматизированной системы. Данный сбой осуществляется целым классом атак типа «Отказ в обслуживании» (DoS-атаки). Таким образом, в первом квартале 2021 года рынок DDoS-атак вырос относительно предыдущего отчетного периода на 40 %. Неожиданный всплеск DDoS-активности можно связать с курсом криптовалют в целом и биткойна в частности [1]. За годы также возросла средняя продолжительность данного типа атак, которая составляет 3 часа. Специалисты в области защиты информации выделяют несколько причин использования DDoS-атак [2]:

- личная неприязнь;
- развлечения;
- политический протест;

– недобросовестная конкуренция;
– вымогательство и шантаж.

DoS-атаки используют уязвимости, которые вызывают сбой целевой системы или службы. Чаще всего такой сбой получается путем насыщения полосы пропускания. Данная атака называется «флудом». Это атака, связанная с большим количеством обычно бессмысленных или сформированных в неправильном формате запросов к компьютерной системе или сетевому оборудованию, имеющая своей целью или приведшая к отказу в работе системы из-за исчерпания системных ресурсов – процессора, памяти или каналов связи.

Дополнительный тип DoS-атаки – это распределенный отказ в обслуживании (DDoS). DDoS-атака происходит, когда несколько систем организуют синхронизированную DoS-атаку на одну цель. Участником данной атаки может быть любое устройство, имеющее выход в интернет. Вредоносные программы попадают на устройства через вложения электронной почты, через загрузку файлов и поддельных программ с непроверенных сайтов. Зараженные устройства организуют сеть под названием «ботнет» [3].

Из класса атак на отказ в обслуживании самой опасной является низкоинтенсивная атака. В отличие от более традиционных атак методом грубой силы, низкоинтенсивные атаки требуют очень небольшой полосы пропускания, и их трудно предотвратить, поскольку они генерируют трафик, который очень трудно отличить от обычного трафика. Наиболее эффективными в данном случае являются системы обнаружения атак, использующие искусственные нейронные сети. Преимущество заключается в постоянном обучении ИНС как на нормальном трафике, так и на аномальном. Искусственную нейронную сеть необходимо обучать на реальных атаках, актуальных примерах, которые производились с использованием существующих популярных инструментов DDoS. Это значительно увеличит шанс распознавания известных и неизвестных DDoS-атак.

На рис. 1 показана схема экспериментального стенда. Для этого была реализована локальная сеть, был добавлен атакуемый объект Apache и его «Оператор». Атакующий трафик исходит от виртуальной машины с Kali. На атакующем объекте, при помощи OracleVirtualBox установлена ОС KaliLinux, где уже предустановлено большинство инструментов для проведения тестов на безопасность. Атакующий трафик генерировался при помощи инструмента slowhttptest. На рис. 2 показаны результаты эксперимента.

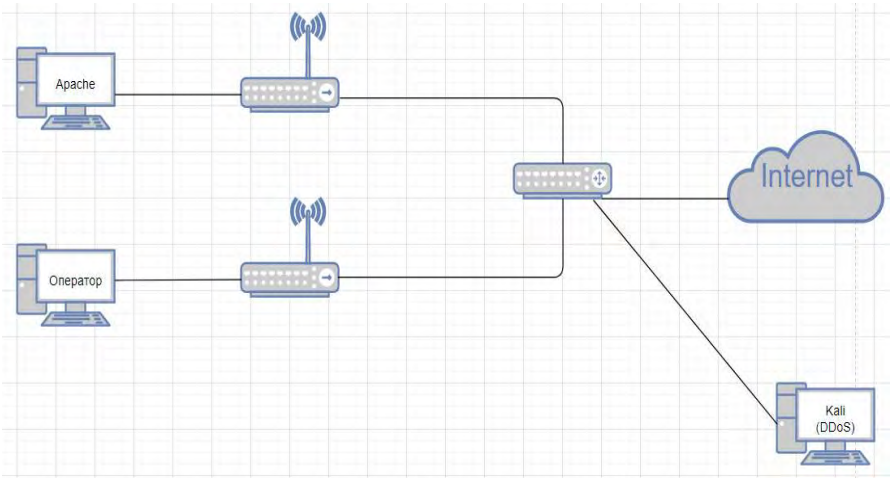


Рис. 1. Общая схема экспериментального стенда

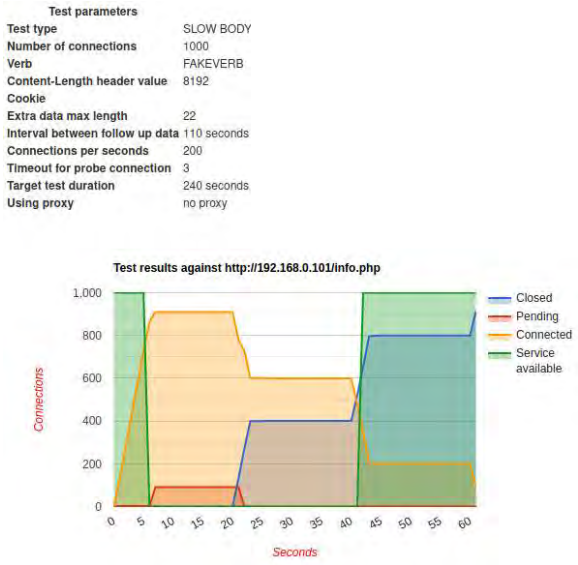


Рис. 2. Результат эксперимента

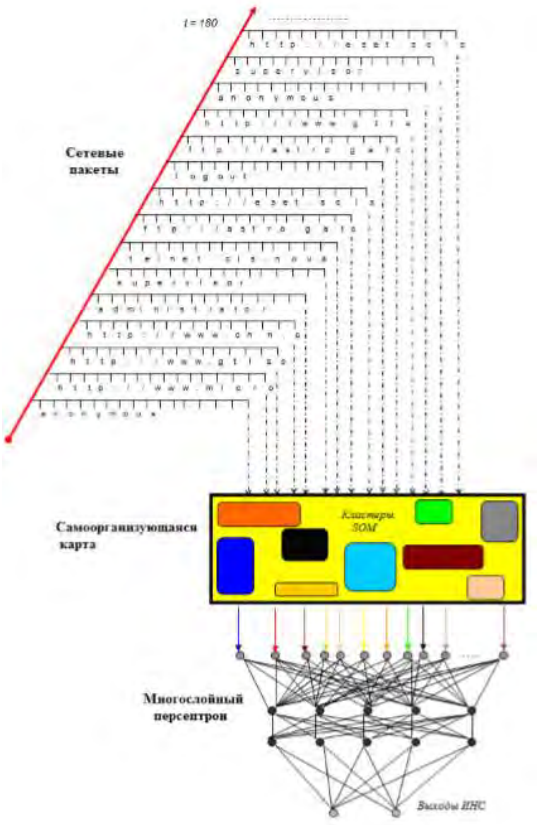


Рис. 3. Архитектура предлагаемой системы обнаружения атак

Для решения данной задачи подойдет ИНС, состоящая из самоорганизующейся сети Коханена (*self-organizingmap*, SOM) и многослойного персептрона (рис. 3), предложенная авторами в научной работе [4].

«При помощи применения карты Кохонена происходит кластеризация 50 символьных событий в узлы матрицы, в которых будут сгруппированы события аналогичных числовых символов. Фактически, отдельные узлы будут представлять собой определённые сценарии атак. После этого данные заголовков пакетов и информация о группировке подаются на вход многослойного персептрона, обученного распознавать аномальный трафик, но

уже с учётом информации о событии, т. е. принадлежности пакета той или иной группе-сценарию. Это позволяет не только обнаруживать аномалии в единичных пакетах, но и выявлять принадлежность пакета к распределённой по времени атаке» [4].

Результаты работы данной системы, предложенные в статье [4], приведены на рис. 4.

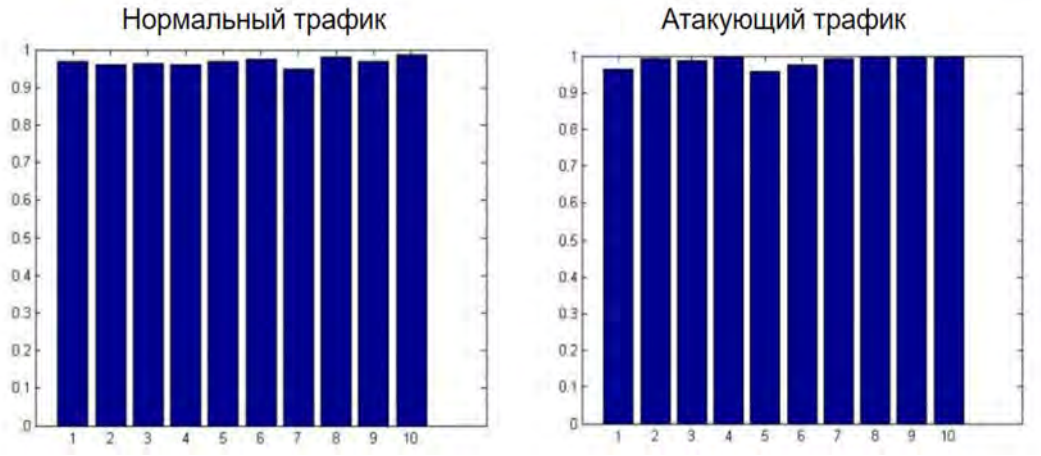


Рис. 4. Результаты распознавания нормального трафика и трафика с атакой

В итоге величина ошибки первого рода (ложное срабатывание) составила 3,16 %. Величина ошибки второго рода (пропуск атаки) составила 1,23 % [4].

В ходе рассмотрения статьи была показана актуальность в необходимости создания современных самобучаемых систем обнаружения атак, а именно, обнаружение низкоинтенсивных атак на отказ в обслуживании. Был проведен эксперимент, рассмотрен один из методов реализации системы информационной безопасности на базе нейросети.

Список используемых источников

1. Отчет «Лаборатории Касперского»: «DDoS-атаки в IV квартале 2020 года». URL: https://securelist.ru/ddos-attacks-in-q4-2020/100469/ (дата обращения 11.05.2021).

2. Абрамов Е. С., Аникеев М. В., Макаревич О. Б. Использование аппарата нейросетей при обнаружении сетевых атак // Известия ТРТУ. 2004. № 1 (36). С. 130.

3. Itglobal.com: «BotNet». URL: https://www.google.com/amp/s/itglobal.com/ru/company/glossary/botnet/amp/ (дата обращения 11.05.2021).

4. Тарасов Я. В. Метод обнаружения низкоинтенсивных DDoS- атак на основе гибридной нейронной сети // Известия ЮФУ. Технические науки. 2014. № 8 (157). С. 47–57. URL: https://cyberleninka.ru/article/n/metod-obnaruzheniya-nizkointensivnyh-ddos-atak-na-osnove-gibridnoy-neyronnoy-seti (дата обращения 11.05.2021).

УДК 004.42
ГРНТИ 50.41.25

МОДЕЛИ УПРАВЛЕНИЯ КАДРОВЫМИ РЕСУРСАМИ В КИБЕРСРЕДЕ ВИРТУАЛЬНЫХ ПРЕДПРИЯТИЙ

С. В. Акимов, Э. Р. Давлетшина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Виртуальные предприятия и организации в настоящий момент времени получают все более широкое распространение, благодаря возможности гибкого управления процессом объединения ресурсов различных партнёров для решения конкретной задачи. Технология виртуальных предприятий и организаций позволяет в кратчайшие сроки создавать географически распределенные временные трудовые коллективы по заданным критериям к их участникам. В статье представлены результаты разработки моделей управления кадровыми ресурсами в киберсреде виртуальных предприятий и организаций на основе электронного портфолио, автоматического вычисления рейтингов и степени соответствия решаемой задаче как отдельных физических лиц, так и трудовых коллективов.

киберсреда, виртуальные предприятия, электронное портфолио, автоматизация, Индустрия 4.0.

Четвертая промышленная революция Индустрии 4.0 обеспечила прорыв в областях роботизации, автоматизации и внедрения киберфизических систем в производственные процессы. Идея формирования единого информационного пространства направлена на сокращение рутинных операций путем их автоматизации, повышение эффективности использования ресурсов для достижения различных целей за счет экономии времени, повышения уровня актуальности и полноты информации [1].

Киберфизические системы стоят на ступени фундаментальных технологических достижений Индустрии 4.0 и являются одной из главных ее компонент. Киберфизические среды активно развиваются, объединяя существующие инфраструктуры со встроенными информационными технологиями – с помощью Интернета, услуг мобильной связи и облачных решений [2].

Виртуальные предприятия становятся новой формой предприятия в постиндустриальном обществе, включающее в себя одно из главных явлений – виртуальная реальность. Все производственные и организационные процессы происходят в киберфизическом пространстве. На основе необходимости создания инициативных трудовых коллективов возникает потребность модернизации и оптимизации данного процесса, в рамках действующих виртуальных предприятий. Возникает вопрос о правильном подборе

кадровых ресурсов по фиксированных компетенциям и рейтинговым отборам для качественного формирования групп специалистов. В настоящее время данная проблема остается открытой для новых идей и разработок.

Одновременно перед участником киберсреды встает вопрос о своей конкурентоспособности и востребованности на рынке труда. В роли системы для контроля за успеваемостью, освоения компетенций, отслеживания результатов научно-исследовательской и профессиональной деятельностей, эффективного планирования и оценивания процесса распределения кадровых ресурсов выступает технология электронного портфолио.

Данные, используемые в электронных портфолио, могут обеспечить участников системы (обучающихся, работников, специалистов, работодателей) эффективными средствами оценки, управления и принятия решений. Таким образом, электронные портфолио предоставляют возможность отслеживать развитие достижений, навыков и компетенций индивида в контексте формального образования, профессиональной подготовки и за его пределами. Эта ключевая характеристика приносит пользу пользователям электронного портфолио, предоставляя им возможность размышлять о своем собственном обучении, саморазвитии, повышении профессиональных навыков [3].

Вопросами по назначению требований к взаимодействию электронного портфолио с другими информационными системами, упрощению обмена и управления данными о компетенциях между различными предприятиями, установлению структуры и целевой функции электронного портфолио занимались такие консорциумы, как IMS Global Learning Consortium Inc., HR-XML Consortium, EuroPortfolio Consortium на базе EIfEL, Inter/National Coalition for Electronic Portfolio Research.

Целевой аудиторией электронного портфолио являются (рис. 1):

– учебные заведения (цель – оценка способностей поступающего, уровня интеллектуального развития, анализ эффективности учебной научной деятельностей; измерение рейтинга компетенций, определение уровня соответствия с требованиями поступления);

– потенциальные работодатели (цель – самореклама, оценка личных качеств, способностей и навыков, оценка профессиональных качеств и умений, уровня компетенции и репутации);

– коллеги, другие пользователи (создание конкурентной среды для стимулирования мотивации в образовании, саморазвитии, повышение самооценки пользователя, поиск единомышленников в профессиональной среде (создание временных трудовых коллективов)).

Рис. 1. Целевая аудитория электронного портфолио

Большую роль играет электронное портфолио физических и юридических лиц в формировании временных трудовых коллективов (ВТК) в рамках виртуальных предприятий. ВТК формируются из высококвалифицированных специалистов, которые отбираются по рейтинговому отбору и компетенциям. Для аутентичного отбора специалистов необходимо использовать современные методы – автоматический подбор персонала по рейтинговым показателям в конкретных областях знаний в рамках системы электронного

портфолио. Такой способ отбора обеспечит быстрое, качественное формирование ВТК для выполнения общей поставленной задачи, выполнения проекта или научно-исследовательской работы.

Электронное портфолио лица представляет собой открытую информационную систему, способную интегрироваться со сторонними информационными системами (например, РИНЦ, Scopus, WoS) для обмена данными методом «одной кнопки». Объектная модель электронного портфолио представляет собой набор взаимосвязанных сущностных классов, представляющие данные по каждому из аспектов информации пользователя.

Результаты интеллектуальной деятельности включают в себя публикации (статьи, книги, монографии, учебные пособия), документы, удостоверяющие исключительное право субъекта на достигнутый им результат интеллектуальной деятельности (патенты, свидетельства о государственных регистрациях) (рис. 2).

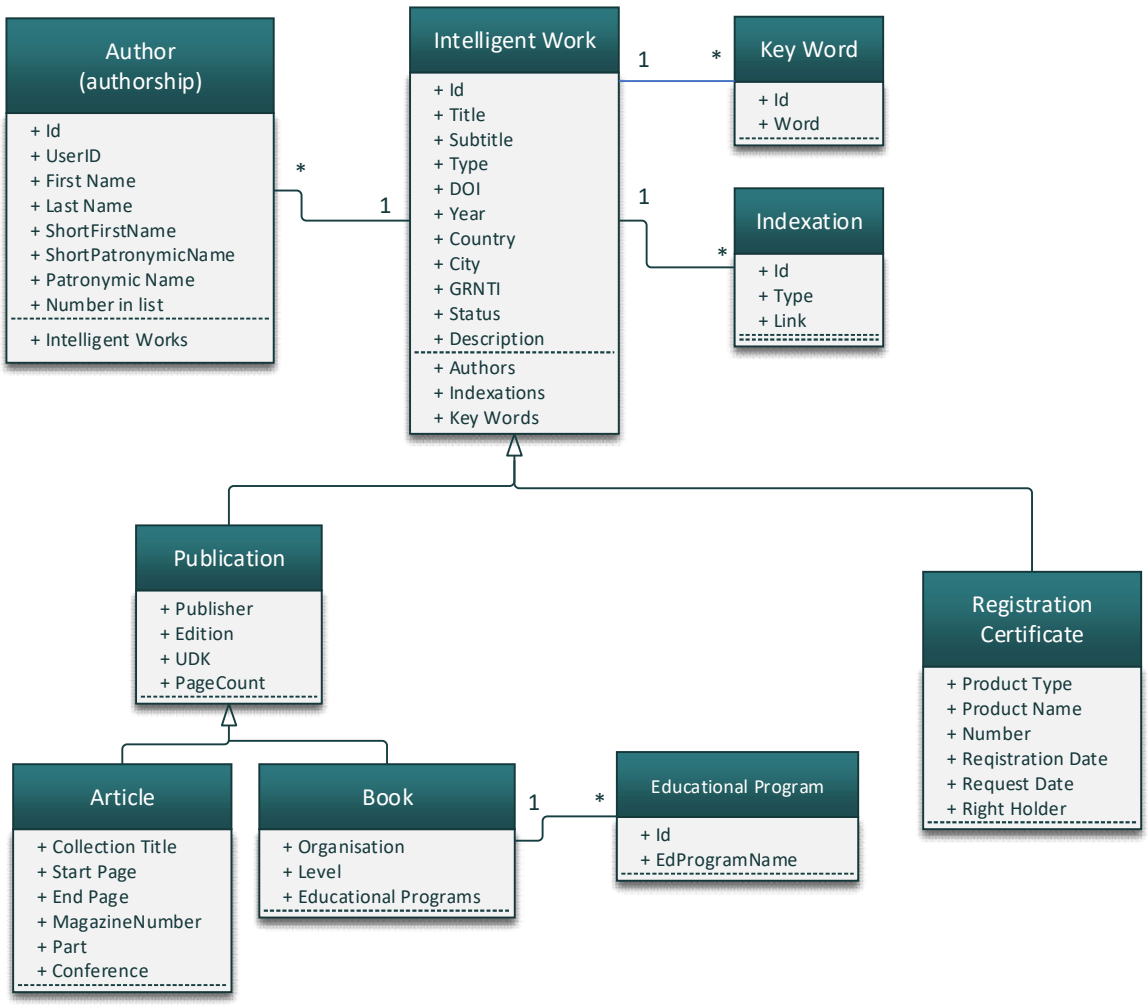


Рис. 2. Диаграмма классов объектной модели электронного портфолио (результаты интеллектуальной деятельности как ключевой аспект)

Личные достижения включают в себя ведомственные награды, участия в конференциях, конкурсах (рис. 3).

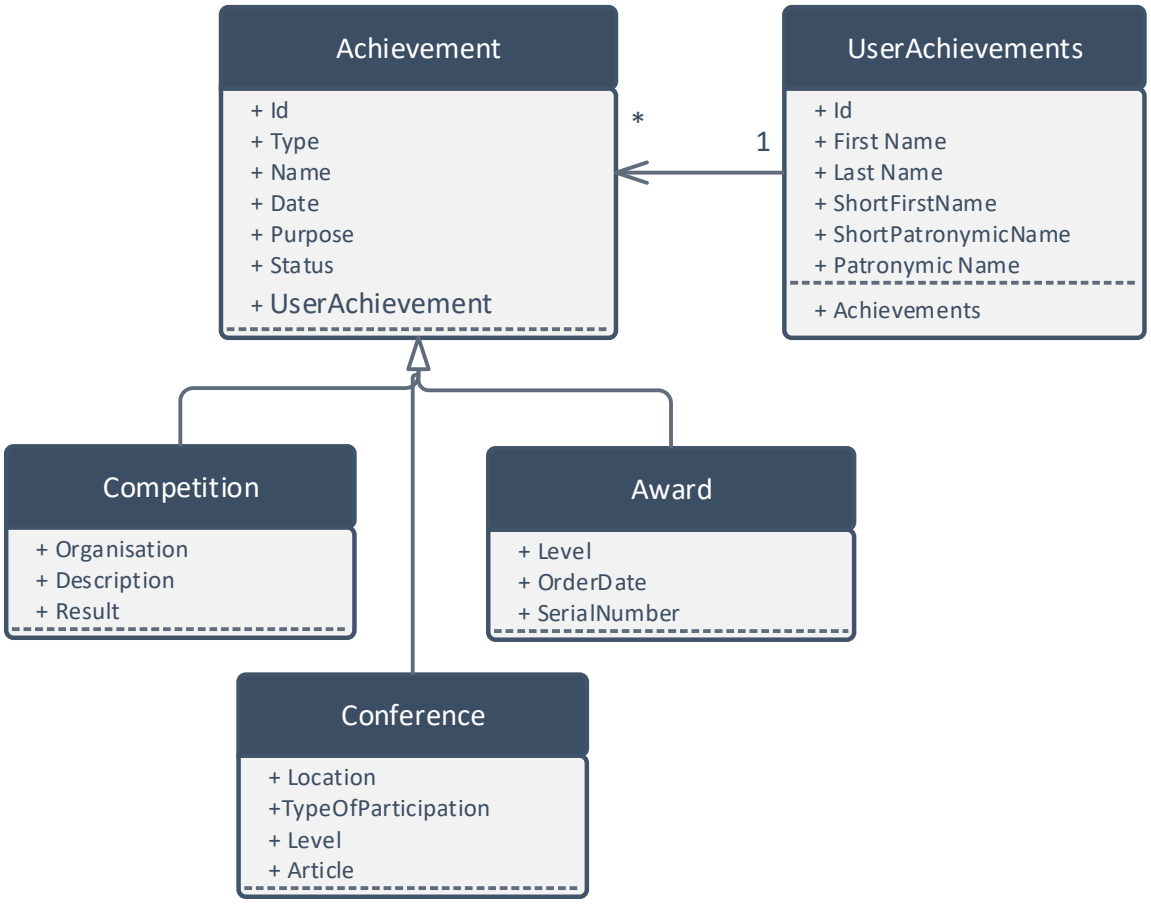


Рис. 3. Диаграмма классов объектной модели электронного портфолио (личные достижения как ключевой аспект)

Внедрение электронных портфолио потенциально может стать эффективным методом отслеживания истории обучения, документирования научно-профессиональной деятельности участников киберсреды виртуальных предприятий, поддержки взаимодействия субъектов между собой, формирования самооценки, а также профессионального развития на рабочем месте.

Список используемых источников

1. Акимов С. В., Верхова Г. В. Формирование киберсреды виртуальных предприятий // Информация и космос. 2016. № 4. С. 89–95.

2. Alp Ustundag, Emre Cevikcan Industry 4.0: Managing The Digital Transformation. Springer Series in Advanced Manufacturing ISBN 978-3-319-57869-9 ISBN 978-3-319-57870-5 (eBook) https://doi.org/10.1007/978-3-319-57870-5.

3. ISO/IEC 20013:2020 Information technology for learning, education and training (ITLET). Reference framework of e-Portfolio information

УДК 004.655.3
ГРНТИ 20.53.17

СПОСОБЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ В ORACLE SQL DEVELOPER

Е. Е. Андрианова, И. А. Липанова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном бизнесе, и вообще, во всех северах деятельности человека, безопасности данных уделяется особое место. Каждая организация должна обеспечить сохранность имеющихся в ней данных. В докладе рассмотрено два способа обеспечения безопасности данных в среде разработки реляционных баз данных Oracle SQL Developer. Первый способ обеспечивается ограничением прав пользователя, при назначении приведений Grant. Второй способ -создание представлений, с помощью которых можно ограничить доступ к конкретной таблице. В докладе приводятся примеры реализации этих способов.

базы данных, безопасность данных, Oracle SQL Developer, реляционная база данных, права доступа.

Все больше и больше растет необходимость в защите данных, это касается любой сферы деятельности человека. Будь то бизнес, образование, медицина и прочее. Учитывая, что на данном этапе развития информационных технологий, практически все данные перенесены на электронные носители и управляются система управления базами данных (СУБД), то и вопрос в обеспечении безопасности в этих СУБД стоит остро. Различные производители таких систем постоянно разрабатывают и совершенствуют способы защиты данных.

В данной статье рассматриваются способы обеспечения безопасности данных в СУБД Oracle SQL Developer.

Для начала следует выделить угрозы, которым подвержены базы данных. К таким угрозам относятся:

– неправомерное использование данных (например, передача данных третьим лицам);

– некорректное внесение данных в базу (избыточность данных или хранение несоответствующее логическим объектам);

– перегрузка базы данных (слишком большой объем хранимой информации, избыточность данных);

– повреждение данных при некорректном использовании БД;

– удаление данных (случайно или злонамеренно).

Исходя из этих угроз следует, что базы данных необходимо защищать с разных сторон, что включает в себя защиту техническими средствами, а также этические и юридические меры. Вопрос доверия к сотрудникам (пользователям базы данных) остается открытым и относится к этике. В данной работе, авторами рассматривается только технические возможности конкретной СУБД.

Первое, что реализуется в каждой СУБД – это обеспечение целостности данных. Целостность данных – это свойство базы данных поддерживать информацию в актуальном, непротиворечивом и безопасном состоянии.

Что бы обеспечить целостность данных в СУБД применяются различные ограничения и правила. Такие правила называются ограничением целостности базы данных. Например, когда речь идет о реляционных и объектно-реляционных базах данных, к которым относится СУБД Oracle SQL Developer, можно выделить такие ограничения целостности:

– создание в каждой таблице первичного ключа, что обеспечивает уникальность каждой записи;

– определение типа и формата поля;

– атомарность хранимых данных (в каждой ячейке);

– разделение хранимой информации на отдельные единицы (таблицы), которые характеризуются предметной областью (обеспечение логической независимости данных);

– правильное соединение таблиц и др.

Все перечисленные способы относятся к организации хранения информация, обеспечивают ее целостность, оберегают от дублирования данных и путаницы, ограничивают ошибки, которые могут допускать пользователи.

Для обеспечения безопасности этих данных с точки зрения злоумышленного использования, следует вводить следующие действия:

– авторизация пользователей;

– разграничение прав пользователей;

– фиксация изменений в БД;

– возможность восстановления данных после сбоев.

По способу доступа к данным, Oracle SQL Developer является клиент-серверной СУБД.

В Oracle SQL Developer можно управлять пользователями как с помощью язака SQl и PL/SQL, а так же при помощи специального интерфейса Database Control, который расположен в разделе Users and Privileges.

Продукты компании Oracle для управления доступом [3]:

- Access management – Защита ИТ-ресурсов и федеративная идентификация для различных сценариев;
- Directory services – Управление крупными каталогами пользователей с быстро выполняющимися операциями «чтение-запись»;

- Database Vault – Контроль доступа привилегированных пользователей по принципу предоставления минимально необходимых прав и разделения обязанностей;
- Label security – Возможность присвоения отдельным записям ярлыков метаданных и предоставление доступа на их основе.

В данной статье, подробно рассматривается способ обеспечения безопасности данных связанный с ограничением прав доступа пользователей. Тут можно выделить 2 основных направления:

1) Ограничение прав для конкретного пользователя;
2) Ограничение доступа к данным для группы пользователей.

В первом случае, при создании пользователя командой create user следует сразу наложить ограничения, либо наоборот, дать права администратора.

На рис. 1 показан пример создания пользователя на языке программирования баз данных SQL, с правами администратора. Как правило, такие привилегии даются администратору базы данных, руководителям и топ менеджерам компании.

```
create user DIRECTOR
identified by secret_pass
account unlock;
Grant DBA to DIRECTOR;
```

Рис. 1. Создание пользователя DIRECTOR

Команда Grant DBA (*Data Base Administrator*) дает пользователю DIRECTOR права администратора базы данных.

На рисунке 2 показан пример создания пользователя, при котором, пользователь имеет четко определенные права, такие как [1]:

- возможность создавать запросы (select) к таблице sales;
- возможность вставлять данные (insert) в таблицу sales;
- возможность обновлять данные (update) в таблице sales;
- возможность удалять данные (delete) из таблицы sales;
- возможность подключаться к сессии.

Привилегии назначаются командой GRANT.

```
create user SELLER identified by SELLER;
grant create session to SELLER;
grant select, insert, update, delete
on SALES to SELLER;
```

Рис. 2. Создание пользователя SELLER

Привилегии бывают системные и объектные, что позволяет обеспечивать безопасный доступ как при подключении к сессии, так и при использовании конкретных объектов.

К системной привилегии относится CREATE SESSION – данная привилегия дает право на подключение к базе данных Oracle, ее можно выдать как конкретному пользователю, так и определенной группе.

Второй способ реализуется в Oracle SQL Developer созданием ролей, это значит, что создаются группы пользователей и каждой из этих групп присваивается определенная роль, включающая в себя определенные права. Например, для разграничения прав доступа, в Политехническом университете созданы роли преподаватель и студент, «преподаватель» включает в себя практически все права администратора, а вот роль «студент» имеет доступ только к некоторым таблицам и может делать только четко определенные манипуляции. При этом, не нужно каждый раз создавая нового пользователя прописывать все права, нужно только присвоить роль.

Так же, ко второму способу можно отнести создание представлений. Представление – это некий образ таблицы, который не хранит в себе данные, а только представляет пользователю их в определенном виде. Представление позволяет дать доступ не ко всей таблице, а только к части данных из нее. Например, имея таблицу «Сотрудник», в которой хранится информация о сотрудниках, такая как ФИО, телефон, дата рождения, паспортные данные, зарплата, надбавка, отдел, необходимо ограничить для секретаря такие данные как информация о зарплате, для этого создается представление, которое будет показывать ФИО, телефон, дату рождения и паспортные данные. В таком случае, для пользователя с ролью «секретарь» будет дан доступ только к представлению, а не к самой таблице с данными. Таким же образом, через представление можно запретить изменение определенных данных в таблице «Сотрудник». На рис. 3 представлен пример создания представления с запретом на изменение отдела.

Если пользователь не оправдал ожиданий и руководитель считает, что нужно закрыть доступ для него к некоторым данным, то применяется команда revoke. На рис. 3 представлен пример, как забрать право на создание запросов к таблице departments у пользователя secretary.

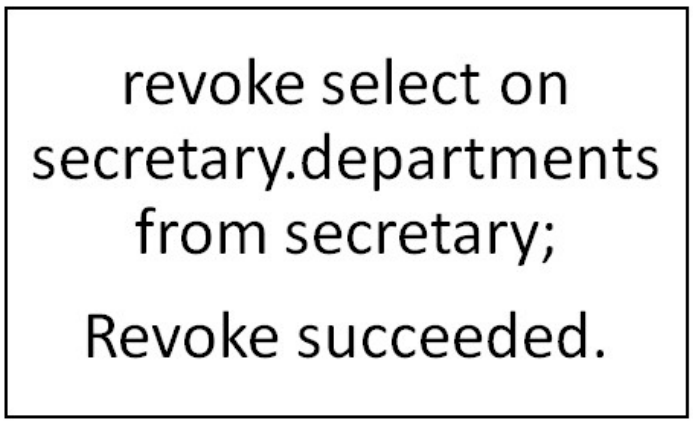


Рис. 3. Отбор привилегии SELECT

Таким образом, в статье было рассмотрено несколько способов защиты данных, которые применяются в СУБД Oracle SQL Developer. Данные в этой СУБД защищены обеспечением целостности и разграничением прав доступа, включая ограничение к представлению данных, к их изменению, удалению и созданию.

Все эти меры направлены на то, чтобы минимизировать, так называемый, человеческий фактор. Они не могут защитить базу данных полностью, невозможно отследить на сколько достоверную информацию вводит пользователь, если говорить о базах с большим объемом хранимых данных, но эти способы позволяют свести риски к некоторому минимуму. В совокупности с такими техническими мерами в организациях применяются и юридические меры, такие как подписание соглашения о неразглашение коммерческой тайны, запрет на передачу персональных данных третьим лицам и прочее.

Список используемых источников

1. Андрианова Е. Е., Селезнева Е. А. Разработка информационной системы для строительной организации в программе Oracle SQL Developer // Студенческая весна – 2020. 74-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых. СПб. : СПбГУТ, 2020. С. 45–49.

2. Андрианова Е. Е., Липанова И. А., Сабинин О. Ю. Интеллектуальный анализ данных для принятия решений в сфере образования // Актуальные проблемы инфотелекоммуникаций в науке и образовании. Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 т. СПб.: СПбГУТ, 2015. Т. 2. С. 1447–1450.

3. Техническая документация на официальном сайте компании Oracle. URL: https://www.oracle.com/a/ocom/docs/gdpr-security.pdf (дата обращения 23.03.2021)

УДК 004.946
ГРАНТИ 28.17.33

ВИРТУАЛЬНЫЕ ТУРЫ НА ОСНОВЕ *3D* ТЕХНОЛОГИЙ

А. В. Аникиева, Е. В. Гунина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В этой статье представлен процесс объединения виртуальных туров и 3D-моделей. Описаны этапы разработки 3D-моделей, с их последующим внедрением в сферические панорамы. Особое внимание уделено актуальности 3D-панорам в разных сферах деятельности. На сегодняшний день виртуальные туры пользуются популярностью среди строительных компаний, архитектурных бюро и рекламных агентств. Также сформулированы идеи по дальнейшим разработкам использования 3D технологий в создании виртуальных туров.

виртуальные туры, 3D, моделирование, графика, 3D-модель, VR, AR, MR, визуализация.

Компьютерные технологии всё активнее используются в различных сферах нашей жизни. *3D* моделирование предоставляет широкий спектр возможностей в детализации и визуализации различных объектов. *3D* графика является незаменимой частью в работе архитекторов, дизайнеров, креативных художников, специалистов по рекламе, специалистов в области игр, медицины и тяжелого машиностроения.

На рынке услуг по презентации объектов недвижимости набирает популярность направление виртуальных *3D* панорам или виртуальных туров. Виртуальные туры – это нечто среднее между статичными рекламными изображениями и полноценной компьютерной игрой, в которой зритель может перемещаться в пространстве, одновременно изучая его особенности, погружаясь в его атмосферу [1]. Виртуальные туры создаются по фотографиям, *3D*-моделям, а также путем комбинирования этих технологий.

Львиная доля того, что человек увидит в виртуальном мире (здания, предметы, техника, фигуры, плоскость, на которой все они находятся), – это *3D*-модели [2]. Существуют разные подходы к их созданию. Основные этапы трехмерного моделирования, из которых состоит любая сцена или объект, представлены на рис.

- 1 этап – это создание объектов и редактирование его составных частей.
- На этапе 2 создаются текстуры и наложение их на *3D*-модель, что определяют ее реалистичность и точность.
- На 3 этапе моделирования с помощью источника освещения создается эффект фотореалистичной картинки. Камера дает возможность зафиксировать угол обзора сцены.

• 4 этап – это результат завершения работы над статичной трехмерной сценой, т. е. файл графического изображения.

Технология виртуальной реальности уже используется в образовательных, развлекательных, маркетинговых, деловых или профессиональных приложениях на компьютере или телефоне [3]. Их можно запускать как на привычных смартфонах, так и на специально разработанных компьютерах со встроенными экранами – очками и гарнитурами.

Рис. Этапы трехмерного моделирования

Благодаря таким приложениям возможно быстро и удобно получать информацию об интересных объектах, просматривать видеоролики или ощущать на себе действия игры, имитирующей реальные ситуации или даже вымышленные вселенные. В зависимости от того, что происходит на экране при открытии приложения, и какое устройство используется, выделяют три вида реальности: дополненная, смешанная и виртуальная.

В дополненной реальности (*augmented reality, AR*) виртуальные объекты проецируются на реальное окружение. Виртуальная реальность (*virtual reality, VR*) – это созданный техническими средствами мир, передаваемый человеку через (пока что) органы чувств. Смешанная (*mixed reality, MR*) или гибридная реальность объединяет оба подхода [4]. Виртуальная реальность создает свой мир, куда может погрузиться человек, а дополненная добавляет виртуальные элементы в реальный мир, т. е. *VR* взаимодействует лишь с пользователями, а *AR* – с внешним миром, следовательно, дополненная реальность меняет мир в режиме реального времени.

Использование технологий *AR* и *MR* позволяют накладывать дополнительные слои графики и голограммы поверх объектов окружающего мира, на которые человек смотрит через камеру телефона или специальных очков. Помимо игр и виртуальной расстановки мебели в реальном помещении, речь может идти о дистанционной примерке одежды, обуви и так далее.

Приложения дополненной реальности подключаются к камере устройства. В случае, если, виртуальные объекты заложены в приложение заранее – то программа как бы «вызывает» их, а затем постоянно перерисовывает картинку в зависимости от угла обзора и взаимодействия с *3D*-моделью [5]. Другими словами, устройство начинает распознавать объекты с камеры и в зависимости от задачи выполняет следующие действия:

– начинает искать дополнительные данные об объекте и выводит их на экран;

– добавляет виртуальные *3D*-модели в ландшафт, интерьер, либо накладывает их на какой-то реально существующий объект.

На сегодняшний день виртуальные туры пользуются популярностью среди строительных компаний, архитектурных бюро, рекламных агентствах, туризме, образовании, а также музеев и так далее [6].

Однако, кроме уже существующих виртуальных туров, предлагается рассмотреть возможность использования туров с дополненной реальностью в таких сферах, как экскурсии по музею или по историческим местам города.

При создании экскурсий по музеям можно использовать технологии *дополненной реальности.* Для воплощения этой идеи необходимо создать *3D*-модель персонажа, посвященного определенной теме или эпохи, в программе *3D*-моделирования, например, с помощью *Autodesk 3ds Max.* Далее *3D*-объекты загружаются в библиотеку приложения, и, при наведении камеры, например, на картину эпохи XVIII века, на экране телефона проецируется один из персонажей картины, который начинает в режиме реального времени рассказывать о событиях и героях данной картины.

Для того, чтобы создать виртуальный тур по городу, *AR* позволяет накладывать *3D*-модели на уже существующий объект и выводить исторические предметы на экран телефона. Прогулка будет более эмоциональна, если при наведении камеры телефона на какой-то исторический или разрушенный объект, на экране они бы по кусочкам принимали первозданный вид в реальном времени.

Если говорить о строящейся недвижимости, то в частичном виде виртуальные туры в этой сфере присутствуют. Но в том объеме, который возможен при современных *3D* технологиях, *AR* и *MR* сделали бы объекты недвижимости привлекательнее и доступнее для потенциальных потребителей. Например, показать, какой вид будет у будущей квартиры, или возможность виртуальной прогулки по готовой квартире.

3D моделирование – это один из мощнейших инструментов по визуализации различных объектов внешнего мира. Виртуальная, смешанная и дополненная реальности могут рассматриваться как перспективное направление. В дальнейшем, необходимы дополнительные исследования для применения и проверки возможностей использования 3D технологий в создании виртуальных туров.

Список используемых источников

1. Виртуальные панорамы. URL: https://ammonit.org/virtualnyie-panoramyi (дата обращения 31.01.2021).

2. Виртуальная реальность. Модуль 4. URL: https://nplus1.ru/material/ 2020/04/24/ VR-chapter-4 (дата обращения 28.01.2021).

3. Виртуальная реальность. Модуль 1. URL: https://nplus1.ru/ material/2020/04/24/ VR-chapter-1 (дата обращения 23.02.2021).

4. Как разработать приложение с использованием VR. URL: https://mdm.ooo/ru/ how-to-develop-a-vr-app/ (дата обращения 31.01.2021).

5. Этапы создания компьютерной игры. URL: https://zen.yandex.ru/media/id/5d4c147cf8ea6700ae4554ba/etapy-sozdaniia-kompiuternoi-igry-5d4fa7513f548700ad0ed0fb (дата обращения 29.01.2021).

6. *3D*-Туры – *3D* визуализация, анимация и моделирование. URL: https://*3D*maximum.com/uslugi/*3D*-tury/ (дата обращения 31.01.2021).

УДК 378.147
ГРНТИ 50.41

ПРИМЕНЕНИЕ КОНТЕЙНЕРИЗАЦИИ В РАМКАХ ПРЕПОДАВАНИЯ ТЕХНИЧЕСКИХ ДИСЦИПЛИН

В. В. Антонов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрены программные варианты реализации контейнеров. Приведено описание создания образов для контейнеров. Предложены варианты конфигурирования контейнеров для использования в практических и лабораторных работах различных технических дисциплин. Раскрыты перспективы применения контейнеризации для построения и изучения технологического стека микросервисных архитектур.

виртуализация, контейнеры, образы, Docker, микросервисы.

Виртуализация информационного пространства экономики особенно в условиях пандемии приобретает решающее значение. Перевод IT-специалистов на дистанционную работу вне офиса ставит задачи по расширенному применению программного обеспечения, обеспечивающего развёртывание бизнес-сервисов в различных виртуальных пространствах. Современное образование не может стоять в стороне от текущих тенденций рынка. В рамках преподавания различных дисциплин в вузе рассматриваются возможности углублённого изучения виртуализации на основе контейнера Docker.

Под виртуализацией понимается набор вычислительных ресурсов, независимых от аппаратной реализации и обеспечивающих изоляцию вычислительных процессов на уровне логики на одном физическом ресурсе.

Контейнеризация (виртуализация на уровне операционной системы, контейнерная виртуализация, зонная виртуализация) – метод виртуализации, при котором ядро операционной системы поддерживает несколько изолированных экземпляров пространства пользователя вместо одного. Эти экземпляры (обычно называемые контейнерами или зонами) с точки зрения пользователя полностью идентичны отдельному экземпляру операционной системы [1].

Сейчас применяются два основных подхода: виртуальные машины и виртуальные контейнеры. Они принципиально различаются тем, что в первом случае для каждой виртуальной машины используется собственный экземпляр операционной системы, а во втором все контейнеры работают с ядром одной операционной системы, но в собственном окружении среды.

Технология контейнеров реализует метод виртуализации на уровне ядра ОС (*operating system-level virtualization*). Вариант подразумевает использование одного ядра хостовой ОС для создания независимых параллельно работающих операционных сред. Для гостевого программного обеспечения организуется только собственное сетевое и аппаратное окружение [1].

Одним из самых популярных стандартов контейнеров является Docker. Docker это целая экосистема открытых проектов. Он позволяет операционной системе запускать процессы в изолированном окружении на базе специально созданных образов (*image*). Образ – это шаблон, который используется для создания контейнеров. Он представляет собой слепок файловой системы, в котором может быть расположен код приложения и развёрнуто специфическое для него окружение. Образ скачивается один раз и в дальнейшем может многократно запускаться и применяться для создания новых образов.

Образы для Docker хранятся в специальном реестре (registry) – публичном репозитории образов (хранилище общедоступно и располагается по адресу https://hub.docker.com).

Docker можно запустить на базе любой операционной системы. При этом размер базового контейнера будет составлять примерно 15 мегабайт. Центральный процессор будет загружен не более, чем на 1–3 %.

Применение контейнеров в преподавании актуально для дисциплины «Операционные системы». В практических и лабораторных работах студенты должны получить навыки работы в различных операционных системах. Установка полноценных операционных систем может оказаться невозможной по причине ограниченности компьютерных ресурсов лабораторий. И тут на помощь может прийти контейнеризация. Для использования в этом учебном курсе можно специально подготовить образы операционных систем со специфическими свойствами или использовать готовые.

Например, для закачивания образа Ubuntu нужно всего лишь выполнить следующую команду:

$> *docker pull ubuntu*

Для запуска этого образа нужно набрать в консоли:

$> *docker run -it ubuntu bash*

При этом возможно указать версию устанавливаемого дистрибутива. По умолчанию устанавливается последняя версия, находящаяся в репозитории.

Существует огромный выбор операционных систем от общеизвестных таких как Debian, OpenSuse, Fedora. Но можно загрузить и использовать и такие экзотические системы как, например, операционная система для роботов (ROS) – это набор программных библиотек и инструментов, которые помогают создавать приложения для роботов. От драйверов до современных алгоритмов и мощных инструментов разработчика – в ROS есть все, что нужно для реализуемого проекта робототехники. И все это с открытым исходным кодом.

Пример последней показанной команды запускает операционную систему с поддержкой утилит командной строки bash, что в свою очередь позволяет изучать различные команды управления операционными системами, например в рамках преподавания дисциплины «Администрирование информационных систем». При этом не существует риска необратимых изменений образов при выполнении студентами работ. Любой образ может быть легко перезапущен в своём начальном состоянии.

Рассмотрим возможность применения контейнеров в следующей дисциплине «Управление данными». Большое количество систем управления базами данных уже находиться в Docker репозитории. Например, СУБД PostgreeSQL.

Для скачивания образа нужно ввести команду:

$> docker pull postgres

для запуска сервера команду:

$>docker run --name some-postgres -e POSTGRES_PASSWORD=mysecretpassword -d postgres.

При этом пользователь и база данных postgres по умолчанию создаются в точке входа с помощью initdb. Одновременно можно указать пароль администратора.

Ещё одни пример команды запуска:

$> docker run -it --rm --name some-postgres --user postgres -e POSTGRES_PASSWORD=123456 -p 5432:5432 postgres

При помощи ключа –name можно задать имя пользователя. Ещё один вариант запуска СУБД представлен ниже:

$> docker run -d -e POSTGRES_USER=postgres -e POSTGRES_PASSWORD=123456 --name my-postgres -p 5432:5432 --restart=always postgres

Два последних примера используют ключ –p, который позволяет выполнить так называемую «проброску портов» на хост машину для управления СУБД.

При необходимости работы с базой данных из специальных графических сред, для PostgreeSQL это утилита администрирования PgAdmin, можно скачать и запустить в контейнере и её.

Команда запуска PgAdmin

$> docker run -p 5050:80 -e "PGADMIN_DEFAULT_EMAIL=antonler@rambler.ru" -e "PGADMIN_DEFAULT_PASSWORD=123456" -d dpage/pgadmin4.

Выполнив в консоли команду *docker ps*, можно получить уникальный идентификатор контейнера, а затем использовать этот идентификатор в команде *docker inspect <dockerContainerId>*. При этом IP-адрес вставляется в pgAdmin и учетные данные базы данных в docker. Например:

$> curl localhost:8080/demo/add -d name=First -d email= antonler@rambler.ru
$> curl localhost:9090/api/v1/add -d engname=teacher -d rusname=%D1%83%D1%87%B5%D0%BB%D1%8C.

Применение контейнеризации в дисциплинах, предполагающих изучение различных методов и технологий разработки программного обеспечения, несколько сложнее. Это обусловлено тем, что необходимо одновременно объединить в один образ несколько различных приложений. Например, разработка web-приложения предполагает наличие базы данных,

веб сервера, и компилятора. И все они должны запускаться одновременно в одном Docker контейнере.

Для создания и публикации собственного образа нужно сделать следующие шаги:

1. Создать Dockerfile, в котором описать процесс создания образа.
2. Выполнить сборку образа командой docker build.
3. Опубликовать образ в Registery командой docker push.

Фал конфигурации Dockerfile имеет простой формат, состоящий из директив и их описаний. Ниже приведён пример конфигурационного файла контейнера для запуска простого Java приложения.

```
#Dockerfile
FROM java:8
ADD FirstApplication.java
RUN javac FirstApplication
EXPOSE 8080
ENTRYPOINT ["java","-jar","/FirstApplication.jar"]
```

Рассмотрим некоторые основные директивы:

FROM – служит для указания образов, от которых происходит наследование контейнера. В данном примере наследуется образ java версии 8. При записи без указания версии устанавливается последняя версия, находящаяся в репозитории.

ADD – добавляет ресурсы в образ, при этом возможно инсталляция целых приложений по аналогии с командой apt get install.

RUN – запускает команды и создаёт слои образа.

CMD – директива служит для указания команд и аргументов внутри контейнера. В примере директива запустит компилятор Java для компиляции файла *FirstApplication.*

ENTRYPOINT – директива, которая будет выполнена при запуске контейнера.

EXPOSE – служит для описания сетевых интерфейсов, которые будут прослушиваться в контейнере. 8080 – это стандартный порт web сервера.

Отдельного рассмотрения требует обучение основам разработки микросервисов. Основной идеологией микросервисов является разделение одного большого монолитного приложения на множество мелких приложений-сервисов общающихся друг с другом при помощи сообщений. В качестве сервисов хорошо подходят акторные модели, описанные в [2]. И здесь на помощь тоже может прийти Docker [3, 4]. Используя файл конфигурации можно прописать и сконфигурировать запуск всех необходимых сервисов. Здесь необходимо отметить, что если количество сервисов доста-

точно большое, то лучше использовать специализированные сервисы и приложения. Сейчас существует целая группа системных приложений для оркестрации контейнеров. Одно из таких приложений это – Kubernetes. Оно позволяет общаться сервисам между собой, запускать и останавливать контейнеры по требованию, запускать дополнительное количество серверов в зависимости от нагрузки.

Преподавание основ контейнеризации в разных дисциплинах позволит развить у студентов целый спектр компетенций, востребованных на современном рынке труда и позволит выпускникам освоить одну из самых высокооплачиваемых IT-профессий DevOps-инженера.

Список используемых источников

1. Колесов А. Виртуализация: технологические подходы // PC Magazine. 2009. № 5. С. 21–22.

2. Антонов В. В. О применении акторной модели примитивов в программных реализациях алгоритмов распознавания образов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. Т. 3. С. 39–43.

3. Моуэт Э. Использование Docker: пер. с англ. М.: ДМК-Пресс, 2017. 354 с.

4. Иан М., Хобсон С. Э. Docker на практике : пер. с англ. М.: ДМК-Пресс, 2020. 516 с.

Статья представлена заведующей кафедрой ИУС СПбГУТ, доктором технических наук, профессором Л. К. Птицыной.

УДК 004.492.3
ГРНТИ 81.93.29

АЛГОРИТМ ВЫЯВЛЕНИЯ ВРЕДОНОСНЫХ ШЕЛЛ-КОДОВ НА ОСНОВЕ СТАТИЧЕСКИХ ЭВРИСТИЧЕСКИХ ПРИЗНАКОВ

М. А. Архипов, Д. О. Маркин

Академия Федеральной службы охраны Российской Федерации

В статье описан алгоритм выявления шелл-кодов на основе статических эвристических признаков для компьютерных систем на основе процессоров с архитектурой ARM. Описано разработанное для демонстрации работы алгоритма программное средство, его структура, тестовые данные для оценки эффективности, модель ВПО для ARM-систем.

полиморфный код, ARM, шелл-код, детектирования, сигнатура, эвристические признаки.

Введение

В настоящее время, в условиях непрерывного насыщения рынка новыми мобильными устройствами наиболее актуальной проблемой информационной безопасности становится обнаружение вредоносного программного обеспечения (ВПО) разработанного под мобильные платформы. Основным разработчиком архитектуры мобильных процессоров является компания *ARM*, которая является лидером за счет оптимального сочетания энергоэффективности и производительности.

Архитектура *ARM* имеет многочисленные специфические особенности [1] по сравнению с распространенными архитектурами *x86/x64*, требующие от исследователей глубокого понимания и компетенций. На данный момент существует потребность детального анализа программного обеспечения (ПО) для компьютерных систем на процессорах с архитектурой *ARM* на предмет наличия недекларированных возможностей, для чего необходимо повысить эффективность известных методов и средств или разработать новые методы и средства выявления уязвимостей.

Проблеме анализа безопасности ПО посвящены многочисленные труды как отечественных, так и зарубежных исследований. Наиболее известные из них труды Гамаюнова Д. Ю. и Сковороды А. А. [2, 3], Гайворонской С. А. [4] и других. Среди иностранных исследователей наиболее известны труды Pinto S. [5], Winter J. [6], Cerdeira D. [7] и других.

Постановка задачи

В связи с особенностями процессорной архитектуры *ARM* разработка программного кода, использующего уязвимости, требует использования определенных команд, характерных только для ВПО. Таким образом, в результате эвристического анализа программного кода вредоносного программного обеспечения, находящегося в открытом доступе, можно выделить такие статические признаки, которые позволят достаточно точно определять наличие недекларированных возможностей в программном обеспечении. При успешном выделении статических признаков возможна реализация статического метода детектирования ВПО, являющегося более быстрым относительно динамического ввиду отсутствия необходимости запускать файл на исполнение.

Модель ВПО

Для реализации вредоносного воздействия злоумышленники часто применяют шелл-коды. Шелл-кодом является набор исполнимых инструкция, осуществляющих эксплуатирование уязвимостей работы с памятью. При реализации алгоритма распознавания признаков шелл-кода предлагается применять сигнатурный метод, основанный на наиболее часто встречающихся признаках, выявленных в ходе изучения исходных кодов доступного ВПО. К таким признакам относятся:

Смена режима работы процессора с *ARM* на *Thumb*. Использования данного метода позволяет злоумышленникам уменьшить объем каждой команды в 2 раза за счет применения в *Thumb*-режиме 16-битных команд, в отличие от 32-битных команд режима *ARM*. Также при смене режима необходимо проследить, чтобы секция *Thumb* была выравнена под 4 байта для исключения ошибок, для этого применяются *nop*-команды, описанные в следующем пункте.

Использование *nop*-команд. *Nop*-команды (англ. *No Operation*) – инструкции процессора, которая предписывает ничего не делать. К *nop*-командам относятся и инструкции, которые в результате выполнения не меняют значения регистров. Данный метод применяются для обеспечения работы вредоносного кода в условиях неизвестности адресного пространства атакуемого узла.

Наличие системного вызова, которому предшествует запись корректного номера системного вызова в определенный регистр (*r7 – для arm32, x8 – arm64*). Признак обуславливается особенностью архитектуры *ARM.*

Алгоритм выявления полиморфных вредоносных шелл-кодов

На основе описанных выше признаков шелл-кодов разработан алгоритм, классифицирующий исполнимые файлы архитектуры *ARM* на легитимное и вредоносное ПО. Для демонстрации работы алгоритма разработано программное средство на языке *Python* 3.

Программное средство производит загрузку анализируемого исполняемого файла в фреймворк для реверс-инжиниринга *radare2,* далее происходит анализ на основе критерия классификации – если в анализируемом файле находится хоть одна сигнатура, соответствующая одному из выделенных признаков, файл классифицируется как вредоносное ПО. В процессе проверки работоспособности алгоритма был произведен анализ тестового набора данных, который состоял из 863 исполняемых файлов для процессорной архитектуры *ARM,* 90 из которых – эксплоиты на основе шелл-кодов из баз данных *www.exploit-db.com, shell-storm.org*, а также шелл-кодов, сгенерированных при помощи средства *ARMSCGen (github.com/alexpark07/ARMSCGen),* 773 – легитимное ПО, полученное

из каталога */bin* микрокомпьютеров *Raspberry Pi* и *Orange Pi.* Структурная схема разработанного программного средства представлена на рис. 1.

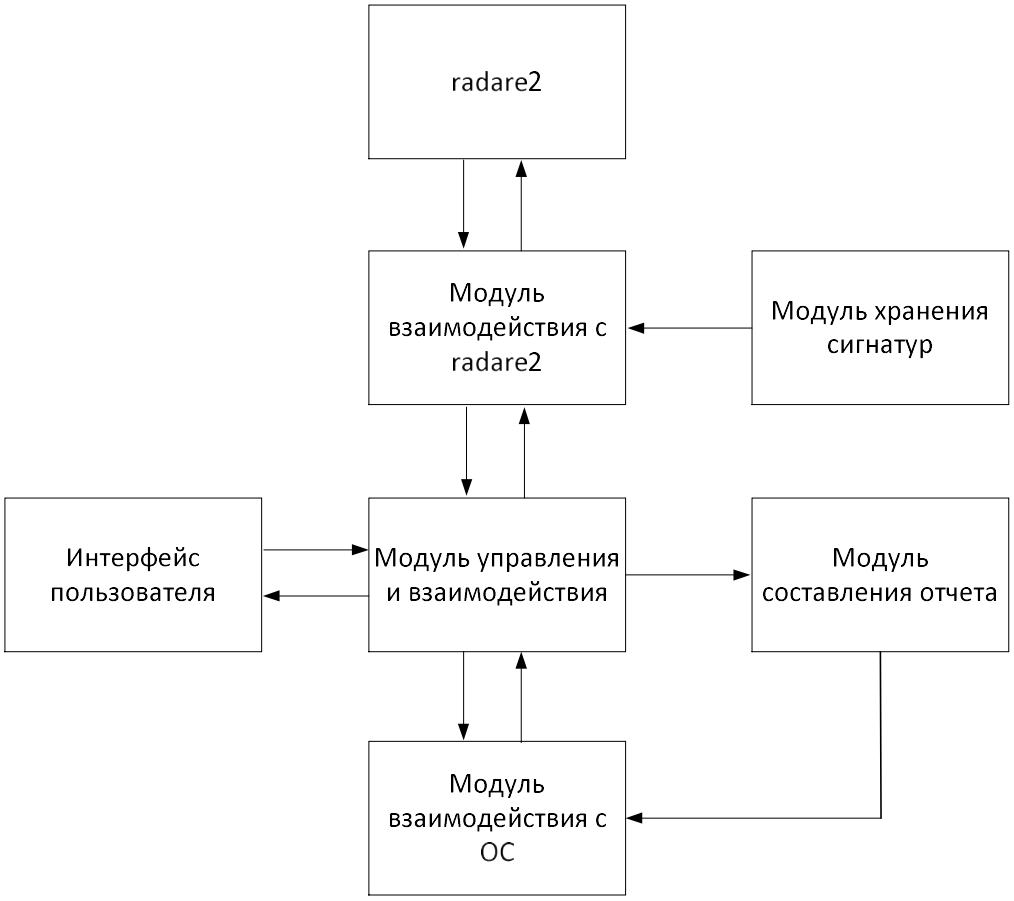


Рис. 1. Структурная схема программного средства

На рис. 2 представлен алгоритм анализа одного *ELF*-файла с помощью разработанного программного средства.

Оценка эффективности

Для оценивания эффективности предложенного алгоритма выявления признаков полиморфных шелл-кодов на основе разработанной модели ВПО была сформирована тестовая выборка бинарных файлов с учетом содержания известных тестовых наборов ВПО и средств их формирования, таких как *Apache-Knacker*, *BID*, *OARC*, *IIS*, *Drebin*, *ISCX*, а также полиморфные вредоносные объекты, формируемые средствами *ADMmutate*, *Metasploit Framework* и эксплоиты, генерируемые: *Metasploit Framework*, *CLET*, *TAPiON*, *Jempiscodes*.

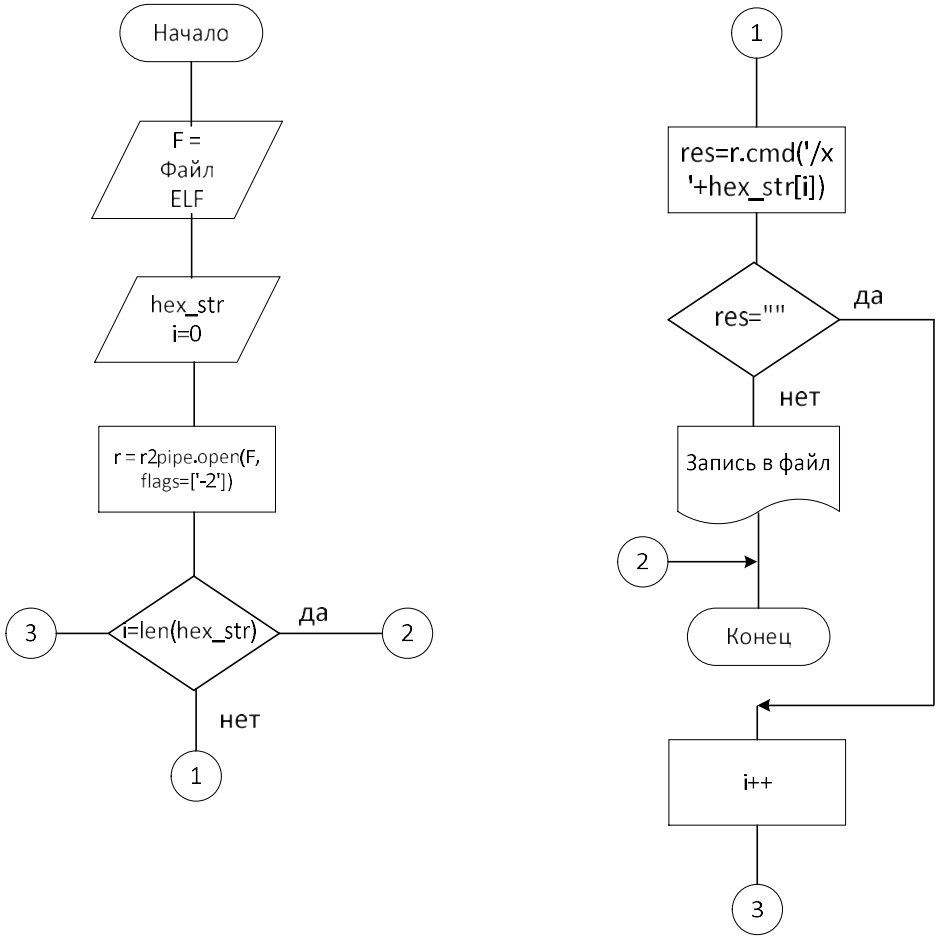


Рис. 2. Алгоритм анализа ELF-файла

Результат работы программного средства представлен в таблице.

ТАБЛИЦА. Оценка эффективности алгоритма распознавания шелл-кодов

Имеющиеся тестовые данные / Результат анализа	ВПО	Легитимное ПО
Детектирован шелл-код	78,9 %	0 %
ELF-файлы	21,1 %	100 %

Выводы

Результат работы алгоритма, представленный в таблице, позволяет оценить разработанный алгоритм обнаружения как эффективный, поскольку в процессе анализа не происходит ложных срабатываний, что подтверждает гипотезу о принадлежности выделенных признаков исключительно к классу вредоносного ПО. При этом выявленные признаки не позволяют однозначно определить наличие шелл-кода в исполнимом файле, так как детектирование произошло только в 78,9 % случаев. Это может быть связано как с внедрением злоумышленником полиморфного кода на этапе

разработки ВПО для затруднения статического анализа, так и с необходимостью выделить новые признаки шелл-кодов для обеспечения полного покрытия. Для обеспечения более эффективного выявления необходимо применить алгоритм динамического анализа исполнимых файлов для архитектуры *ARM,* который позволит детектировать вредоносный полиморфный программный код.

Анализ особенностей функционирования ДСИ в современным *ARM* процессорах позволяет сделать вывод, что адаптация технологии *TrustZone* для нужд отечественной экономики за счет применения подходов по повышению доверия к ней, включая сертификацию и разработку отечественного ПО на основе *TrustZone*, является важным направлением совершенствования отечественных технологий обеспечения безопасности информации в условиях отсутствия производства достаточного количества элементной базы. Особенно, учитывая количество современных устройств, в основе которых лежат процессоры с архитектурой *ARM*.

Список используемых источников

1. Маркин Д. О., Умбетов Т. К., Архипов М. А., Миначев В. М. Современные технологии построения доверенных сред исполнения приложений на уровне базовой системы ввода-вывода // Безопасные информационные технологии : Десятая международная научно-техническая конференция : сб. трудов (Москва, 3–4 декабря, 2019 г.). М.: МГТУ им. Н.Э. Баумана, 2019. 409 с. : ил. – С. 281–286.

2. Гамаюнов Д. Ю., Сковорода А. А. Анализ мобильных приложений с использованием моделей привилегий и API-вызовов вредоносных приложений // Прикладная дискретная математика. 2017. № 36. С. 84–105. doi http://doi.org/10.17223/20710410/36/7.

3. Гамаюнов Д. Ю., Сковорода А. А. Динамический анализ мобильных приложений // Программная инженерия. 2019. № 7-8. С. 324–333. doi http://doi.org/10.17587/prin.10.324-333.

4. Гайворонская С. А., Гамаюнов Д. Ю. Гибридный метод обнаружения шелл-кодов // Системы высокой доступности. 2012. Том 2, № 8. С. 33–44.

5. Pinto, S.; Santos, N. Demystifying Arm TrustZone: A Comprehensive Survey // ACM Computing Surveys, 2019. January 10. p. 36.

6. Winter, J. Experimenting with ARM TrustZone – Or: How I met a friendly piece of trusted hardware // Proc. of the IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, 2012. Pp. 1161–1166.

7. Cerdeira, D.; Santos, N.; Fonseca, P.; Pinto, S. SoK: Understanding the Prevailing Security Vulnerabilities in TrustZone-assisted TEE Systems // Conferense IEEE Symposium on Security and Privacy, San Francisco, CA, January 2020. p. 17.

УДК 004.9
ГРНТИ 50.05.09

ИССЛЕДОВАНИЕ МЕТОДОВ ОПТИМИЗАЦИИ ИГР В МЕЖПЛАТФОРМЕННЫХ СРЕДАХ РАЗРАБОТКИ (НА ПРИМЕРЕ UNITY)

М. М. Архипова, А. В. Фёдорова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Материал посвящен рассмотрению различных методов оптимизации игр, разрабатываемых с помощью программного обеспечения Unity. В процессе создания игр становится актуальным вопрос обеспечения высокого уровня их работоспособности на различных устройствах. Задача оптимизации состоит в том, чтобы при минимальном количестве затраченных ресурсов получить максимальный прирост производительности. Будут рассмотрены основные методы решения данной задачи, и выявлены их особенности, позволяющие использовать их при реализации проектов в среде разработки Unity. Также будет предложен ряд рекомендаций, способствующих улучшению оптимизации игр, создаваемых с использованием рассматриваемой межплатформенной среды разработки.

Unity, оптимизация игр, частота кадров в секунду, кеширование, статический батчинг, динамический батчинг.

Оптимизация игры – это процесс повышения производительности для улучшения игрового процесса и визуального восприятия. Если конкретнее, то хорошо оптимизированная игра работает с одинаковым FPS на большинстве игровых платформ, включая технические слабые модели. Такой подход к оптимизации, где исходная точка – FPS (частота кадров в секунду), неудивителен, т. к. большинство игроков связывают производительность игры именно с плавностью отображения картинки на экране [1]. Ведь большую часть информации мы получаем визуально.

Показателем степени оптимизации игры является частота кадров в секунду (FPS). Такой подход выбран не случайно, ведь большую часть информации мы получаем визуально. Чем выше частота кадров в секунду, тем более плавно отображается картинка на экране. Хорошо оптимизированная игра должна работать с одинаковым FPS на большинстве игровых платформ, включая технически слабые модели.

Рассмотрим метод оптимизации игр под названием batching (пакетирование). Его смысл заключается в группировке аналогичных задач обработки. Например, если вам нужно сделать покупки, вы не ходите в магазин

и обратно за каждым отдельным товаром. Вместо этого вы составляете список товаров, идете в магазин и покупаете все за одну поездку. Метод работает аналогичным образом. Это помогает оптимизации, создавая гораздо меньше работы для визуализации одной и той же графики. Потенциально в каждом кадре отображаются сотни графических элементов, что делает пакетирование одним из основных принципов оптимизации [2].

Статический батчинг (*static batching*) используется в том случае, когда игровые объекты статические [3]. Такие объекты не должны перемещаться, масштабироваться или вращаться, а также должны использовать один и тот же материал, тогда батчинг будет работать. Тип объекта можно выбрать в окне Inspector, пример указан на рис. 1.

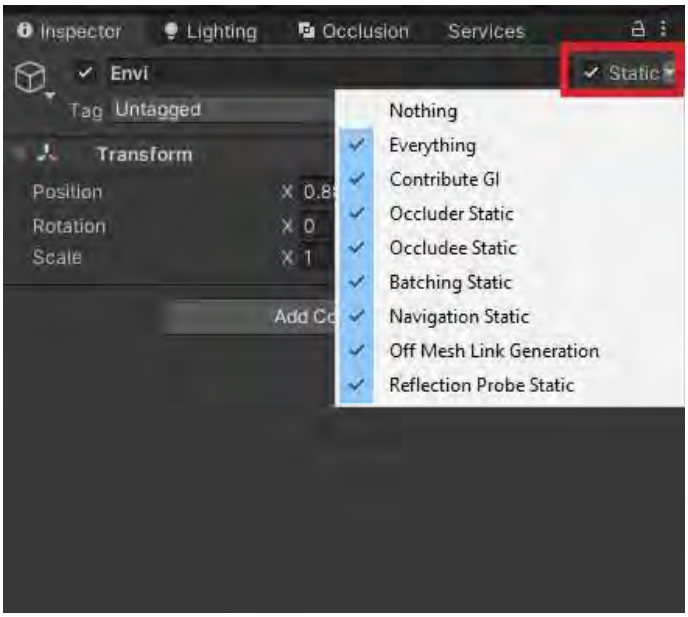


Рис. 1. Выбор типа объекта

Динамический батчинг (*dynamic batching*) похож на статический в том, что для игровых объектов должны использоваться те же материалы, но может группировать движущиеся объекты без необходимости делать их статическими [3]. Данный метод используется для объектов, которые будут перемещаться. Подобно static batching, он будет сочетать элементы с подобными материалами.

Ещё один способ повышения производительности – кэширование. Метод включает в себя временное хранение данных, поэтому они могут быть доступны более быстро для повторного использования. Для понимания принципа его работы предположим, что вы находитесь в магазине и забыли положить несколько предметов в свой список. Вместо того, чтобы звонить домой, чтобы напомнить о каждом элементе, вы звоните один раз и записываете элементы (кэш), поэтому информация есть, когда вам это нужно. Кэшируйте все, к чему вам часто приходится получать доступ [3].

Увеличить производительность игры может также оптимизация 3D-моделей. Высокодетализированные объекты сильно нагружают железо. Поэтому не желательно использовать полигонов больше, чем нужно, а также следует уменьшать количество швов на UV-карте и жёстких рёбер, которые удваивают вершины [4]. Редукция полигонов – это упрощение 3D-модели с помощью уменьшения количества полигонов. Принцип простой: группа полигонов заменяется одним. Пример представлен на рис. 2.

Также на производительность влияет освещение в игре. Генерация реалистичных лучей света, их отражение от поверхности и создание теней – один из самых ресурсоемких процессов. Поэтому разработчики зачастую избавляются от теней на больших расстояниях и стараются использовать как можно меньше отражающих свет текстур. Уменьшение числа объектов с динамичными тенями также положительно сказывается на повышении производительности игры [5].

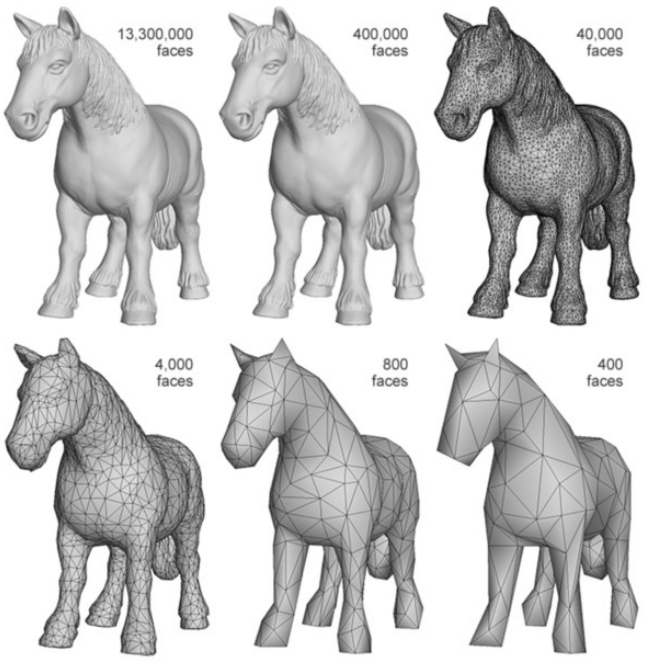


Рис. 2. Уменьшение количества полигонов

Следуя данным советам, вы сможете добиться значительного уменьшения запросов прорисовки, а также оптимизировать без лишних затрат ваш проект. Желательно задуматься об оптимизации вначале работы над вашим проектом, поскольку в дальнейшем это может стать сложнее. Нужно понимать, что оптимизация игр – это работа не только над графикой, но и над игровыми механиками, избавление проекта от багов, корректная локализация и множество других нюансов. Работа над улучшением производительности игры важна не менее, чем процесс создания её создания.

Существует ещё множество индивидуальных способов улучшить производительность игры, характерных для определенного жанра или стиля, но общий обзор настроек производительности поможет вам независимо от типа создаваемой игры.

Список используемых источников

1. Как работает оптимизация игр? URL: https://club.dns-shop.ru/blog/t-64-videoigryi/37130-kak-rabotaet-optimizatsiya-igr/ (дата обращения 25.03.2021).

2. Оптимизация производительности графики. URL: https://docs.unity3d.com/ru/530/Manual/OptimizingGraphicsPerformance.html (дата обращения 25.03.2021).

3. Introduction to Optimization with Unity. URL: https://learn.unity.com/tutorial/introduction-to-optimization-in-unity# (дата обращения 25.03.2021).

4. Рекомендации по производительности для Unity. URL: https://docs.microsoft.com/ru-ru/windows/mixed-reality/develop/unity/performance-recommendations-for-unity (дата обращения 29.03.2021).

5. Советы: как оптимизировать 3D-игры. URL: https://vc.ru/playgendary/120585-optimization (дата обращения 30.03.2021).

УДК 004.056.53
ГРНТИ 81.93.29

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ С ПРИМЕНЕНИЕМ СЕТЕВЫХ АНАЛИЗАТОРОВ И ТЕСТОВ НА ПРОНИКНОВЕНИЕ

М. Э. Ахметшина, Р. М.-А. Манкаев, И. А. Ушаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современный мир уже невозможно представить без гаджетов, быстрого доступа в Интернет и других современных устройств, которые люди привыкли использовать каждый день. Они становятся незаменимыми атрибутами нашей жизни, которые сопровождают человека в повседневности: как в быту, так и на рабочем месте. Все процессы в современном обществе перетекают в информационные системы, которые играют центральную роль в обеспечении эффективности работы коммерческих, государственных предприятий и образовательных организаций. Широкое использование информационных систем, которые применяются для хранения, обработки и передачи информации, обуславливает актуальность проблемы защиты и сохранности информации в них.

аудит информационной безопасности, снифферы, сетевой трафик, Snort.

Введение

В настоящее время стали появляться многочисленные проблемы, относящиеся к достоверности и анонимности информации [1, 2]. Чтобы обеспечить ее безопасность пришлось прибегнуть к созданию такого программного обеспечения, с помощью которого можно осуществить анализ сетевого трафика для обнаружения проблем, связанных с утечкой данных или взломом компьютерных сетей, возобновление всех потоков данных сети, а также анализ статистики сетевых данных для изучения аномальности трафика.

Для успешной работы и выявления всех проблем информационной безопасности, анализ трафика должен быть проведен в полном объеме, чтобы обеспечить применение всех методов анализа для достижения эффективного результата.

Одним из способов проникновения в компьютерные системы является эксплуатация уязвимостей. Этот способ эффективен благодаря наличию неисправленных уязвимостей в широко используемом программном обеспечении. Кроме того, некоторые пользователи и компании не устанавливают дополнения и обновления, закрывающие известные уязвимости в приложениях.

1 Общие сведения об аудите информационной безопасности

Аудит информационной безопасности – это интегративный процесс получения непредвзятых качественных и количественных оценок о текущем состоянии информационной защищенности автоматизированной системы в соответствии с установленными критериями и показателями безопасности [3].

С помощью аудита можно оценить: насколько безопасно функционирует информационная система, прогнозировать риски и обоснованно подойти к вопросу обеспечения безопасности информационных активов, стратегических планов развития и в целом содержимого ценной корпоративной информации.

Аудит безопасности информационных систем состоит из следующих этапов [4]:

1. Инициирование проведения аудита.
2. Сбор информации.
3. Разбор полученных данных.
4. Выработка рекомендаций.
5. Подготовка отчетов.

2 Характеристика современных инструментов анализа сетевого трафика

Тестирование на проникновение (пентест) – это метод оценки безопасности компьютерных систем и сетей с помощью моделирования атаки злоумышленника [5]. Этот процесс включает в себя анализ системы на наличие уязвимостей, которая может вызвать некорректную работу системы. Анализ ведется с позиции потенциального атакующего и может включать в себя активное использование уязвимостей системы. Испытание на проникновение является частью аудита безопасности. Можно выделить наиболее популярные области применения сетевых анализаторов:

– анализ трафика для обнаружения проблем в работе сети (в том числе, несанкционированной активности);
– воссоздание потоков данных («прослушивание»);
– предотвращение различного рода сетевых атак;
– сбор статистики.

Если говорить о комплексном решении задачи анализа сетевого трафика, то в первую очередь следует разделить ее на три автономные подзадачи (рис. 1): перехват трафика, его хранение и анализ.

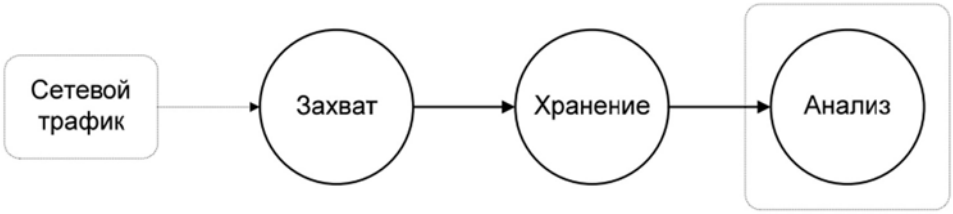


Рис. 1. Подзадачи системы анализа сетевого трафика

Система анализа должна гарантировать 100 % захват трафика, а также предоставлять результативные методы анализа и навигации по его результатам. Захват трафика реализовывается с помощью снифферов. В общем случае, сниффер – это программа или программно-аппаратное устройство, которое предназначено для перехвата трафика. Сниффер может быть установлен как на маршрутизаторе, так и на конечном узле сети (рис. 2).

Рис. 2. Схема сети с использованием сетевого анализатора

В практической части работы используется сетевой анализатор Snort [6]. Здесь анализ трафика основан на механизме сигнатурного поиска.

3 Установка и настройка сетевого анализатора в режиме обнаружения вторжения

Для получения оповещений о несанкционированном доступе к информационным ресурсам системы используется выбранный сетевой анализатор.

Откроем файл local.rules для настройки правил фильтрации пакетов, проходящих через Snort. В этом файле следует прописать желаемые правила фильтрации и захвата пакетов.

После перезапуска программы в режиме обнаружения вторжений укажем «показать тревоги». Произведем попытку сканирования портов с атакующего компьютера. Видим, что в консоли «Snort» вывелось предупреждение о попытке сканирования (рис. 3).

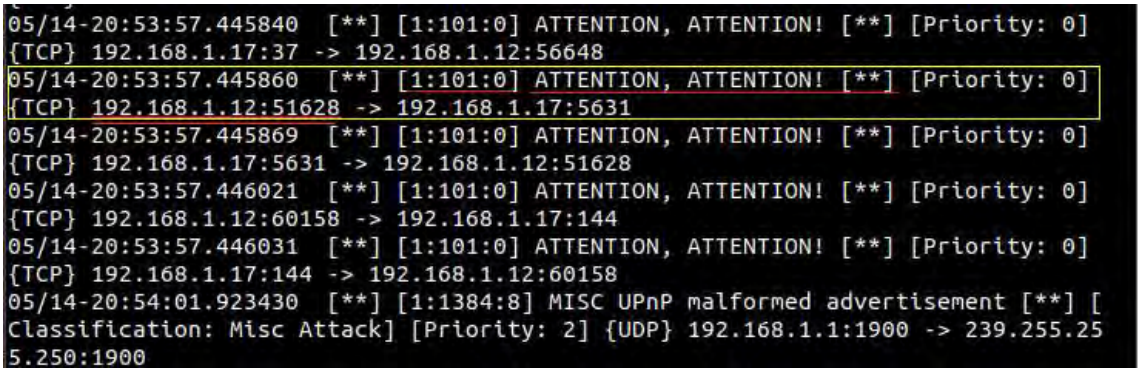


Рис. 3. Реакция «Snort» на сканирование

Здесь можно увидеть IP адрес атакующего.

4 Реализация работы сетевого анализатора в режиме предотвращения вторжения

Сетевой анализатор справился с задачей обнаружения аномальной активности в сети. Но в современных реалиях не всегда вовремя удается отреагировать на обнаруженную устройством атаку. Для устранения данной проблемы задается новое правило, в котором при совпадении заданного сценария, например, при обнаружении ICMP пакетов, программа автоматически блокирует этот трафик (рис. 4). Таким образом, Snort будет настроен в режиме не только обнаружения, но и предотвращения атаки.

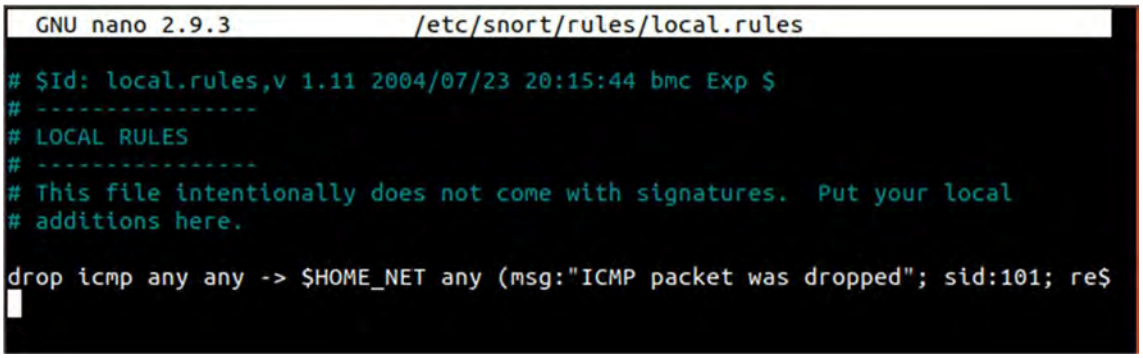


Рис. 4. Пример правила фильтрации пакетов

Запустим Snort в режиме предотвращения атаки с выгрузкой результатов в файл для удобства чтения. Попробуем послать пинг-запросы с атакующей машины.

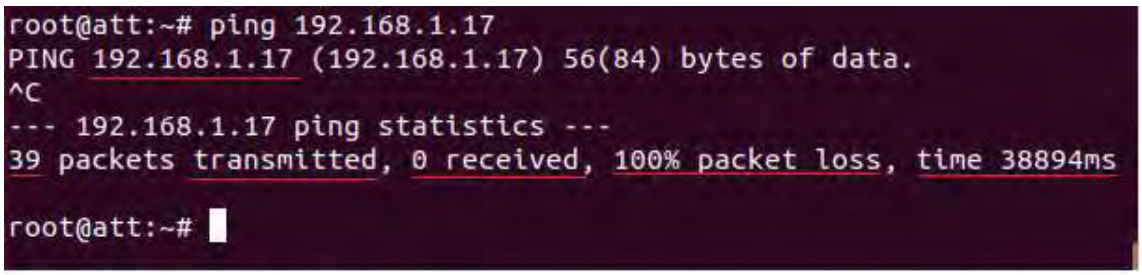


Рис. 5. Результат выполнения пинг-запроса

После продолжительного времени производится остановка выполнения команды. Как видно на рис. 5, 39 пакетов были отправлены и ни один не вернулся. Это означает, что система предотвращения атаки сработала.

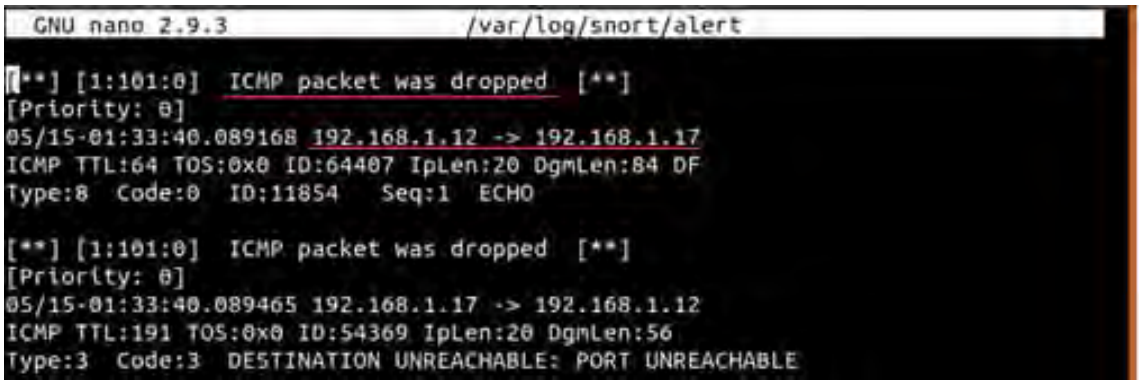


Рис. 6. Содержимое файла с результатом проведенной операции

Snort успешно зафиксировал попытку отправки ICMP пакетов в сеть, вывел заданное сообщение и заблокировал их по предписанному правилу (рис. 6). С помощью такого способа можно задавать множество различных и гибких правил, необходимых для настройки системы безопасности.

Заключение

В данной работе был описан принцип проведения аудита информационной безопасности, рассмотрены современные технологии проникновения в защищаемую систему. Изучены характеристики инструментов анализа сетевого трафика.

Установлен сетевой анализатор и настроен с помощью сигнатурных правил фильтрации пакетов, что позволило моментально получить сигнал о вторжении в защищаемую систему. Следом была проведена попытка отправки пакетов, где был четко отображен результат успешного обнаружения атаки с помощью сетевого анализатора.

В результате разработан алгоритм обнаружения и предотвращения атаки с использованием анализатора сетевого трафика и сигнатурных правил фильтрации в нем. С помощью такого способа можно задавать большое

количество различных и гибких правил, необходимых для конкретной системы. Использование данного алгоритма автоматизированного обнаружения и предотвращения атак позволит перераспределить нагрузку на средства защиты информации и повысить комплексную безопасность информационной системы.

Подводя итог, учитывая тенденции и темпы развития информационных технологий, существующие методы проникновения в защищаемую систему из-за создания и совершенствования новых способов передачи информации и применяемых технологий будут только требовать доработки и улучшаться, поэтому данная проблема никогда не перестанет быть актуальной.

Список используемых источников

1. Kaspersky News: итоги 2018 года. URL: https://www.kaspersky.ru/about/press-releases/2018_according-to-kaspersky-lab-in-2018-half-of-computers-at-industrial-enterprises-in-russia-faced-cyber-threats (дата обращения 01.11.2020).

2. Kaspersky Security Bulletin 2019. Статистика. URL: https://securelist.ru/kaspersky-security-bulletin-2018-statistics/92906/ (дата обращения 01.11.2020).

3. Вайнштейн Ю. В., Демин С. Л. Основы информационной безопасности: Учебное пособие. Красноярск, 2014. 270 с.

4. Стандарт Банка России СТО БР ИББС-1.1-2007 «Аудит информационной безопасности» от 28 апреля 2007 г. № Р-345.

5. ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология, 2019 г. 3 с.

6. Snort. URL: http://www.snort.org/ (дата обращения 14.11.2020).

7. Nmap. URL: https://nmap.org/ (дата обращения 14.11.2020).

УДК 004.891.2
ГРНТИ 20.23.17

ПРИМЕНЕНИЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОГНОЗИРОВАНИИ ФИНАНСОВОГО СОСТОЯНИЯ КРЕДИТНЫХ ОРГАНИЗАЦИЙ

А. В. Бабаева, В. Л. Литвинов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Финансовая стабильность банковского сектора во многом зависит от эффективного банковского регулирования и надзора. Качество превентивного банковского

надзора зависит от качества прогнозирования финансовых показателей кредитных организаций. При выборе модели прогнозирования финансовых показателей следует учитывать ряд особенностей, которые присущи финансовому сектору, например, таких, как глубина исторических данных и необходимость экспертной интерпретации результатов. При моделировании следует также учитывать как факторы из внутренней отчетности банка, так и внешние – из отчетности других банков и различные макроэкономические показатели. Правильное построение модели системы с использованием искусственного интеллекта, её валидация, а также постоянный мониторинг рисков модели позволит достигнуть максимальных результатов в области прогнозирования финансового положения кредитных организаций.

банковский надзор, анализ финансового состояния кредитных организаций, интеллектуальные системы поддержки принятия решений, банковский сектор, линейная регрессия, прогнозирование.

Информационные системы и технологии – неотъемлемая часть финансового сектора. С целью повышения эффективности взаимодействия с финансовыми рынками в новой цифровой среде Банку России также целесообразно применять цифровые технологии для упрощения и повышения качества функций, связанных с исполнением регуляторных требований.

Эффективное банковское регулирование может быть обеспечено системой прогнозирования показателей деятельности кредитных организаций и планирования соответствующих мер надзорного реагирования. Актуальность решения данных задач особенно возрастает в условиях экономических кризисов, поскольку наличие эффективных превентивных мер банковского надзора и регулирования позволяет оперативно выявлять существенные проблемы и обеспечить «вывод с рынка» кредитных организаций с неустойчивым финансовым положением [1].

Выбор модели следует рассматривать с учетом входным данных задачи, для которой она будет применяться.

Динамика баланса банка представляет собой типичный авторегрессионный процесс. Если использовать для моделирования исходный ряд, высока вероятность выявить сложную зависимость с факторами [2].

Наиболее простым и стандартным подходом решения задач прогнозирования балансовых показателей является линейная регрессия с оценкой параметров методом наименьших квадратов [4]. В общем виде метод наименьших квадратов формулируется следующим образом:

$$F(x, y, a, b) = \sum_{\mathrm{i}=1}^{\mathrm{n}} (a + bx_i - y_i)^2 \longrightarrow \min,$$

где a, b – коэффициенты линейной регрессии,

n – количество анализируемых периодов,

x_i – наблюдаемые значения независимой переменной (в нашем случае, это – время),

y_i – наблюдаемые значения зависимой переменной (прогнозируемый показатель).

Коэффициент b представляет собой средний прирост прогнозируемого показателя за рассматриваемый временной период, который нам необходимо найти для того, чтобы построить прогнозное значение по следующей формуле:

$$y_{T+\tau} = y_T + b\tau,$$

где y_T – фактическое значение прогнозируемого показателя в момент времени T,

$y_{T+\tau}$ – прогнозное значение показателя в момент времени, отстоящий на τ временных интервалов от последнего фактического значения.

Независимая переменная (время) принимает некоторые дискретные значения, обычно рассматриваемые как 1, 2, 3, …, n. С учетом этого, общее уравнение метода наименьших квадратов может быть переписано в следующем виде:

$$F(y, a, b) = \sum_{i=1}^{n} (a + bi - y_i)^2 \longrightarrow \min.$$

Предполагается, что целевая переменная – прирост баланса, представляет собой линейную комбинацию из определенных факторов с некоторой нормально распределенной шумовой компонентой.

Функция потерь может быть представлена в виде квадрата разности фактической целевой переменной и модельной:

$$L(w) = \sum_{i=0}^{n} (w * x_i + b - y_i)^2.$$

Задача минимизации функции потерь заключается в нахождении условий равенства вектора параметров линейной регрессии произведению обратной ковариационной матрицы факторов на матрицу факторов и на вектор целевой переменной.

Если факторы линейно зависимы, их ковариационная матрица будет необратима, и, соответственно, решения не будет.

Если факторы сильно скоррелированы, мультиколлинеарны, то при расчете обратной матрицы в знаменателе будут значения, близкие к нулю.

В таких случаях будет наблюдаться очень сильная неустойчивость оцененных значений коэффициентов.

Одним из способов регуляризации является регуляризация Тихонова, которая в общем виде выглядит как добавление нового члена к среднеквадратичной ошибке:

$$L(w) = ||x^T * w - y||^2 + \lambda * ||w||^2,$$

Суть данного подхода заключается в том, что мы в функцию потерь вносим добавку, зависящую от размера коэффициентов и некоторого параметра λ. Тогда при минимизации функции минимизируется и размер коэффициентов. Для выбора оптимального значения параметра λ обычно используется либо метод контрольной выборки, либо кросс-валидация [4].

Прогнозирование показателей доходности может также осуществляться методом наименьших квадратов. Однако для данных показателей существует определенная особенность – периодичность представления. Отчетность, которая является входными данными для расчета показателей доходности согласно Указанию Банка России от 3 апреля 2017 года № 4336-У «Об оценке экономического положения банков», представляется кредитными организациями в Банк России раз в квартал. Данный фактор значительно снижает количество наблюдений [3].

Для прогнозирования показателей капитала в надзорных целях особо важное значение имеют показатели на последние отчетные даты, соответственно метод наименьших квадратов может быть модифицирован следующим образом:

$$F(x, y, a, b) = \sum_{i=1}^{n} \left(\frac{i}{n}\right)^3 (a + bx_i - y_i)^2 \longrightarrow \min,$$

где выражение $\left(\frac{i}{n}\right)^3$ обеспечивает эффект «затухания». Под «затуханием» понимается снижение в разумных пределах чувствительности модели метода наименьших квадратов с тем, чтобы присвоить больший вес последним наблюдениям.

Существуют и другие подходы к оценке параметров модели, например, подход, основанный на формуле Байеса. В некоторых случаях он может дать существенное преимущество в сравнении с линейной регрессией. Подход Байеса основан на одноимённой формуле [3]:

$$P(B|A) = \frac{P(A|B) * P(B)}{P(A)},$$

где *P(B|A)* – вероятность наступления события «*B*» при условии наступления события «*A*»;

P(A|B) – вероятность наступления события «*A*» при условии наступления события «*B*»;

P(A) – вероятность наступления события «*A*»;

P(B) – вероятность наступления события «*B*».

Есть несколько методов численной оценки параметров при данном подходе. В настоящее время наиболее популярным является метод Монте-Карло на основе Марковских цепей. Существует множество алгоритмов, которые генерируют оценочные распределения на основе данного метода, они отличаются по сложности реализации, требуемой вычислительной мощности и точности.

После выбора метода и построения модели, следует проводить первичную оценку критериев качества. Используемые методы должны соответствовать поставленным задачам. Также должен быть определен спектр ограничений, которые возникают при применении данной модели.

Определение наиболее подходящей модели и постоянный ее мониторинг на всех стадиях жизненного цикла модели позволит достигнуть максимальной эффективности при прогнозировании финансовых показателей кредитных организаций.

Список используемых источников

1. Липанова И. А., Ильяшенко О. Ю., Андрианова Е. Е. Информационные технологии. Поддержка принятия решения. Обработка данных: учебное пособие / рец.: О. Ю. Сабинин, Т. Ю. Ковалева; Федеральное агентство связи, Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". СПб.: СПбГУТ, 2014.

2. Андрианова Е. Е., Липанова И. А., Сабинин О. Ю. Управление данными. Интеллектуальный анализ данных: учебное пособие / рец.: О. Ю. Ильяшенко, Е. В. Давыдова ; Федер. агентство связи, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". СПб.: СПбГУТ, 2016.

3. Ветров Д. П., Кропотов Д. А. Байесовские методы машинного обучения: учебное пособие. Москва, 2007. 67 с.

4. Уткин В. Б. Эконометрика: учебник. 2-е изд. М.: Дашков и К, 2017. 21 с.

УДК 004.353, 004.
ГРНТИ 20.50.21, 20.53.33

ПРЕДСТАВЛЕНИЕ ОРГАНИЗАЦИИ ДОПОЛНЯЮЩИХ УСТРОЙСТВ ОТОБРАЖЕНИЯ СИТУАЦИОННОГО ЦЕНТРА

И. Ю. Баранов, А. А. Панов, И. И. Скоробогатов

Академия Федеральной службы охраны Российской Федерации

Предлагается представление организации дополняющих устройств отображения в ситуационном центре для повышения эргономических свойств зала заседаний за счет перераспределения на них низкодинамичной информации организационного и информирующего характера, обеспечивающей снижение дефицита сведений об окружающем пространстве и обсуждаемых тем.

ситуационный центр, система отображения, модель организации.

Введение

В общем случае в ситуационный центр (СЦ) подается неформализованная и формализованная информация различного представления. Выдача всего информационного потока без его структурирования будет отвлекать лиц, принимающих решения (ЛПР). В условиях ограниченного времени участников совещания и/или ЛПР важным фактором эффективной работы СЦ является время, затраченное на восприятие информации и принятие решений [1].

Дополняющая (вспомогательная) информация в зале заседания СЦ может выполнять следующие информативные функции:

– анонс оперативных событий и объявления;

– напоминание о следующем событии;

– информирование о докладчике, теме его выступления;

– фамилия, имя, отчество участника конференции, выступающего в прениях или задающего вопрос докладчику, номер его микрофона и др.;

– информирование о следующем докладчике и/или докладе;

– таймер отсчёта времени выступления для докладчика;

– длительность перерыва;

– указание направления при перемещении участников совещания;

– краткое информирование о различных фактах, событиях, явлениях;

– напоминание о следующем событии;

– отображение температуры и других актуальных для данного момента данных.

Как отмечено в [2], дополняющая информация в СЦ обладает малой информативностью, невысокой динамичностью демонстрации и небольшим объемом данных (одно предложение или фраза) по сравнению с основным содержательным материалом совещаний. Такая информация совместно с основным информационным потоком позволит снизить дефицит сведений об окружающем пространстве СЦ и обсуждаемых на заседании тем.

Представление организации дополняющих устройств отображения СЦ

Для организации дополняющих устройств отображения (ДУО) предлагается применение информационных панелей [3] и их конфигурирование на основе различного набора светодиодных модулей, собранных на базе светодиодных матриц и использующих клиент-серверную модель взаимодействия [4]. Размещение ДУО должно быть увязано с планом помещения и порядком проведения совещаний, что позволит повысить эргономические свойства зала заседаний (совещаний) СЦ. Здесь важным является соответствие места размещения ДУО той информации, которая на них отображается [2]. Например, логичным является размещение сведений о выступающем за трибуной докладчике непосредственно на самой трибуне, к которой приковано внимание участников совещания. Варианты размещения таких ДУО в зале заседаний СЦ (пример представления зала заседаний СЦ взят из [5]) показаны на рис. 1.

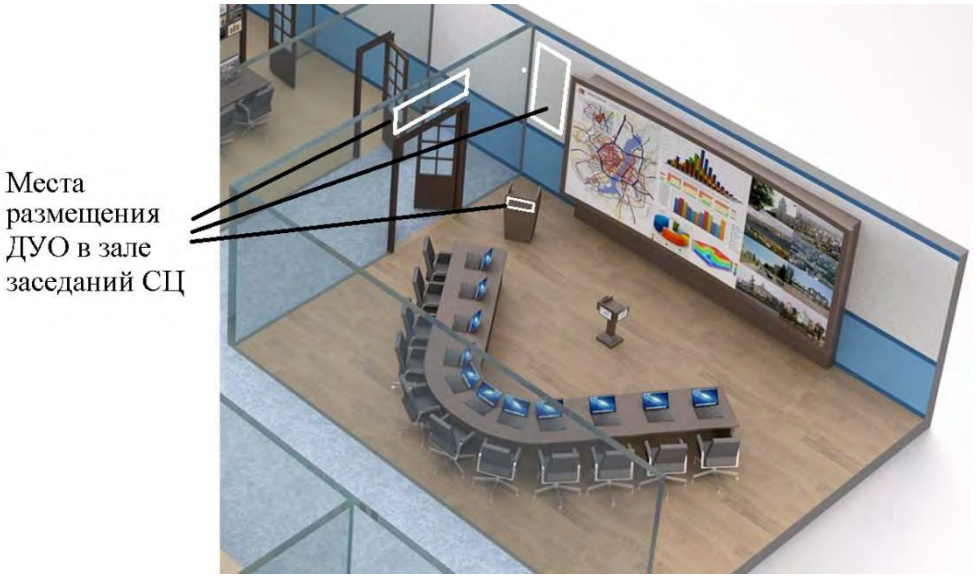


Рис. 1. Варианты размещения ДУО в зале заседаний СЦ

Для оценки возможности использования в качестве технической основы ДУО исследованы характеристики применяемых в настоящее время устройств отображения информации – телевизоров и мониторов на основе

различных технологий (LED, OLED, плазменная и т. д.), проекторов, светодиодных экранов, видеокубов и др. Результат выбора светодиодных экранов в качестве ДУО обусловлен следующими преимуществами по сравнению с другими типами устройств отображения:

– возможность конфигурирования размера под конкретные условия размещения и формат представления информации на экране;

– относительно невысокая стоимость;

– возможность работы в асинхронном режиме (без подключения к управляющему компьютеру);

– выше яркость и контрастность (лучше видно в большего расстояния);

– наличие готового программного обеспечения для оперативного управления и настройки;

– подключение к сети в качестве удаленно управляемого устройства типа IoT (Internet of Things – интернет вещей).

Представление организации светодиодного экрана на основе панелей, состоящих из модулей светодиодных матриц, с системой асинхронного управления показано на рис. 2.

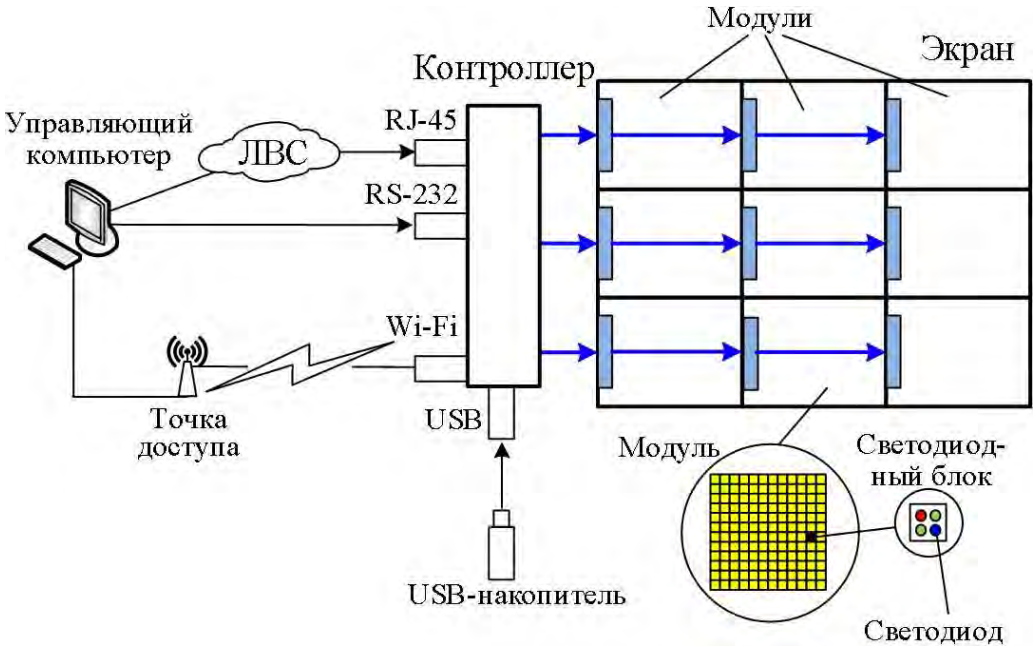


Рис. 2. Модель организации светодиодного экрана с системой асинхронного управления

Режимы работы ДУО

В асинхронном режиме информация на экран переносится посредством удаленной или локальной записи в память контроллера светодиодного экрана. Файлы для демонстрации на экране передаются в этот контроллер посредством интерфейсов USB, Ethernet, Wi-Fi или RS-232, после чего он зацикливает всю полученную информацию и может воспроизводить ее

непрерывно. ДУО состоит из панелей (кабинетов), состоящих, в свою очередь, из нескольких светодиодных модулей и контроллеров, количество которых определяется размерами экрана. Асинхронная система управления позволяет светодиодному экрану работать автономно без участия управляющей ЭВМ, а также, при необходимости, оперативно перезаписывать в память контроллера ДУО новый блок информации. В качестве управляющей ЭВМ может быть выбран любой компьютер локальной сети с установленным специализированным программным обеспечением, кроме того, он же может управлять несколькими ДУО. После записи файлов в контроллеры светодиодных экранов, этот компьютер может использоваться для других целей, не связанных с управлением ДУО.

В отличие от асинхронного в синхронном режиме на светодиодном экране демонстрируется та же информация, что и на экране управляющего компьютера. При этом управляющий компьютер должен использоваться только для этих целей, что для низкодинамичной информации нецелесообразно с экономической точки зрения.

Для нетребовательных к объему отображаемой информации условий сборку небольшого экрана упрощают, используя только модули светодиодных матриц без привязки к панелям (кабинетам) светодиодного экрана типовых размеров. Данные модули представляют собой наборы светодиодных блоков, изготовленных по классической схеме RGB (красный, зеленый и синий) из 3-х, иногда 6-ти светодиодов для отображения одного пикселя. Разрешение такого экрана обычно кратно 8, 16, 32 или 64 пикселям. Например, для вывода дополняющей (вспомогательной) информации в виде текстового блока, в котором указана фамилия, имя и отчество выступающего докладчика, достаточно размера ДУО в 32x128 пикселей и с шагом пикселя от P4 до P8.

Методика настройки ДУО в асинхронном режиме работы

В асинхронном режиме на скорость обновления информации на светодиодном экране влияет способ передачи данных. При первом способе используется локальный интерфейс USB и USB-накопитель. Необходимо на любой пользовательский компьютер установить специализированное программное обеспечение (ПО), с помощью которого формируется файл с информационными блоками (фото, видео, текст и др.) и сценарием их демонстрации. Затем этот файл с помощью flash-накопителя переносится в контроллер светодиодного экрана. Во втором случае контроллер ДУО подключается к локальной сети и передача информации в него осуществляется напрямую. Методика настройки для второго способа представляется следующим образом:

1 этап: установка на управляющем компьютере специализированного ПО для светодиодного экрана в соответствии с инструкцией к нему;

2 этап: настройка сетевого адреса ДУО с помощью данного ПО (установка IP-адреса в контроллере ДУО);

3 этап: подготовка информационных блоков требуемого формата (разрешения) с использованием информационных ресурсов управляющего компьютера или локальной сети;

4 этап: формирование сценария демонстрации информационных блоков на экране;

5 этап: передача информационных блоков в контроллер ДУО без остановки отображения предыдущего изображения.

Выводы

Предложение по организации дополняющих устройств отображения в СЦ позволяет повысить эргономические свойства зала заседаний СЦ за счет размещения низкодинамичной информации организационного и информирующего характера, обеспечивающей снижение дефицита сведений об окружающем пространстве и обсуждаемых на заседании тем.

Список используемых источников

1. Кукушкин А. А. Сетецентрическая парадигма развития ситуационных центров: монография. Орёл: Академия ФСО России, 2014. 163 с.

2. Baranov I. Y., Panov A. A., Skorobogatov I. I. Improvement of the model of information flows of the situation center due to complementary display devices // Modern informatization problems in technological and telecommunication systems analysis and synthesis (MIP-2020'ES): Proceedings of the XXV-th International Open Science Conference (Yelm, WA, USA, January 2020). Yelm, WA, USA : Science Book Publishing House, 2020. Pp. 219–223.

3. Новикова Е. В. Создание ситуационных центров на базе аудиовизуальных и информационно-коммуникационных технологий : материалы конференции «Ситуационные центры: модели, технологии, опыт практической реализации». М. : РАГС, 2006. 25 с.

4. Белоус К. В., Вачугова В. А. Разработка информационной панели на базе светодиодных матриц // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. тр. СПб.: СПбГУТ, 2018. Т. 2. С. 63–67.

5. Визуализация информации. Каталог 2010–2011. М.: Полимедиа, 2010. 113 с.

УДК 621.396.4
ГРНТИ 49.03.11

ОПРЕДЕЛЕНИЕ ИНФОРМАТИВНОЙ ЗНАЧИМОСТИ ТРЕБОВАНИЙ К ПОКАЗАТЕЛЯМ КАЧЕСТВА ТЕХНИЧЕСКОЙ ОСНОВЫ СИСТЕМЫ УПРАВЛЕНИЯ СВЯЗЬЮ

А. С. Башкирцев, И. Б. Паращук

Военная академия связи

Рассмотрен подход к решению задачи определения объема и номенклатуры требований к показателям качества технической основы системы управления связью. Этот подход позволяет получить оценки относительной информативности требований, а также основан на многокритериальном ранжировании по информативности исходной совокупности требований, описывающих систему при ограничениях на ресурсы для достижения требуемой результативности процесса автоматизированного управления связью.

связь, управление, техническая основа, требования, система, показатель качества, информативность, матрица, значимость.

Техническая основа системы управления связью (ТОСУС) является базой соответствующей автоматизированной системы. При этом автоматизированная система управления связью (АСУС) представляет собой комплекс аппаратных средств, программных средств и персонала, предназначенный для управления различными процессами в рамках обеспечения пользователей услугами связи. Поиск и разработка адекватных методов, позволяющих сформулировать требования к современной ТОСУС, с учетом эволюции в телекоммуникациях, является, по-прежнему, актуальной задачей [1].

Актуальность этой задачи также объективно связана с тем, что существующие методы обоснования требований к современной ТОСУС, как правило, используют математические методы аддитивной свертки и методы параметрической и структурной декомпозиции. Данные методы имеют ряд преимуществ, но не позволяют адаптивно, в динамике совершенствовать систему требований к ТОСУС в случае изменения требований системы управления к системе связи, что, в конечном итоге, приводит к необходимости разработки новой системы таких требований.

Таким образом, на наш взгляд, своевременной и значимой выглядит задача разработке методического аппарата, обеспечивающего определение

требуемой номенклатуры и объема требований, а также учитывающего особенности эксплуатации ТОСУС и разработки ее элементов.

Учитывая, что задача оптимизации номенклатуры и объема системы показателей качества (ПК) ТОСУС и процесса автоматизированного управления связью, является задачей сокращения размерности множества данных с помощью выявления определенного числа основных факторов, размерностей, кластеров и т. д., которые могут объяснить изменчивость результативности АСУС, ее решение может и должно строиться на основе математических методов редукции с учетом наличия корреляционных связей между показателями качества (параметрами).

Иными словами, в основе формулировки задачи лежит вопрос – существует ли возможность построения на имеющемся множестве показателей качества (параметров) сколько-нибудь разумной и полезной системы их отношений с состоянием ТОСУС и процесса автоматизированного управления связью. Причем, построение таких отношений возможно на основе формулировки соответствующих моделей, которые ориентированы на традиционные задачи классификации.

Известно, что классификация является своеобразной «сверткой» исходных информационных признаков, поскольку число идентифицируемых классов всегда меньше, чем уникальных объектов. Иными словами, в итоге получается небольшое по размеру, наглядное и рациональное представление данных (признаков) в пространстве существенно меньшей размерности, чем исходное. Именно поэтому математические методы редукции пространства признаков (требований) являются одним из наиболее эффективных средств решения задач классификации и ранжирования.

Одним из современных подходов к решению задач классификации и ранжирования является подход, в основе которого реализуются механизмы ранжирования по информативной значимости. Ранжирование требований к ПК по информативной значимости позволяет снять неопределенность наблюдаемого (моделируемого, описываемого) состояния ТОСУС, которая количественно характеризуется энтропией этого состояния [2].

Предположим, что вектор требований $\vec{Q}_{<m>}$ полностью определяет облик ТОСУС. Тогда, используя описанное в работах [3, 4] свойство, заключающиеся в том, что энтропия совокупности независимых величин равна сумме энтропии этих величин, справедливо записать:

$$H_{\Sigma} = \sum_{m=1}^{s} H_m(Q), \qquad (1)$$

где H_{Σ} – энтропия состояния ТОСУС,

$H_m(Q)$ – безусловная энтропия m-го требования.

При этом количество информации о состоянии ТОСУС (информативность) $I_m(Q_m, \Sigma)$, которую несет *m*-е требование, можно записать:

$$I_m(Q_m, \Sigma) = H_\Sigma - H_m(\Sigma / Q_m), \quad (2)$$

где $H_m(\Sigma / Q_m)$ – условная энтропия состояния ТОСУС после задания требования Q_m.

Первый важный аспект определения информативной значимости требований к ПК – формулировка и задание требований к современной ТОСУС следует начинать с требования Q_m, которое «несет» максимальное количество информации $I_m^{\max}$, при этом энтропия по *m*-му требованию определяется в соответствии с выражением [4]:

$$H_m(Q) = -\int_{-\infty}^{+\infty} f(Q_m) \log_2 f(Q_m)\, dQ_m, \quad (3)$$

где $f(Q_m)$ – функция распределения по *m*-му требованию. Так как функция распределения $f(Q)$ почти всегда определяется как многоугольник вероятностей, выражение (3) может быть представлено в виде [3, 4]:

$$H_m(Q) = -\sum_1^n p_i \log_2 p_i, \quad (4)$$

где p_i – вероятность совпадения требования Q_m с *i*-м интервалом диапазона его значений.

Второй важный аспект определения информативной значимости требований к ПК ТОСУС – требования можно выбирать по критерию минимума величины энтропии. При этом, поскольку распределение $f(Q_m)$ почти всегда подчинено нормальному закону, энтропия отдельного требования, согласно (3), равна [4]:

$$H_m(Q) = -\frac{1}{\sqrt{2\pi D_{Q_m}}} \int_{-\infty}^{+\infty} \left[\exp\left(\frac{Q_m^2}{2D_{Q_m}} \right) \right] \left(-\frac{1}{2} \log_2 2\pi D_{Q_m} - \frac{Q_m^2}{2D_{Q_m}} \log_2 2\pi D_{Q_m} \right) dQ_m, \quad (5)$$

где D_{Q_m} – дисперсия m-го требования.

Физический смысл выражения (5) состоит в упорядочении требований по степени информативности, причем это упорядочение осуществляется по величине дисперсии распределения требований. Очевидно, что меньше

дисперсия требований D_{Q_m}, тем плотнее распределение и тем больше вероятность того, что требования принадлежат к одному классу, характеризующему определенное состояния ТОСУС. Чем больше дисперсия требований D_{Q_m}, тем менее коррелированными являются задаваемые требования к ПК ТОСУС с результативностью управления.

Этот метод может быть использован при вероятностном прогнозировании результативности функционирования ТОСУС, когда идентифицируются и оцениваются значения дисперсий подпроцессов прогнозируемого процесса автоматизированного управления связью.

Полученное в результате упорядочения требований и их выбора по степени информативности суммарное количество информации, которое содержит совокупность задаваемых требований (Q_1,Q_2, …,Q_m), может быть представлено в виде [4]:

$$I_s(\mathrm{z}_s, \Sigma) = I_{z_1} + I_{z_2} + \ldots + I_{z_s}. \qquad (6)$$

В результате упорядочения требований и их выбора по степени информативности, с учетом влияния требований к ПК ТОСУС на результативность автоматизированного управления связью, может быть получена матрица относительной информативной значимости требований к ПК ТОСУС.

После определения относительной информативной значимости каждого требования, осуществляется реорганизация модели зависимостей. При этом относительно требования с наибольшим значением *I*, матрица делится на две части таким образом, что столбцы, в которых отмечена зависимость свойств от данного требования, переносятся в левую часть, другие в правую. В дальнейшем рассчитывается относительная информативность применительно к сформированной матрице.

При этом относительная информативность на втором шаге определяется как сумма относительной информативности левой и правой части матрицы зависимостей. Проведение итерационных вычислений позволяет провести ранжирование требований относительно их информативной значимости. Расчеты показывают, что уже на седьмом шаге итераций значения относительной информативности требований становится неразличимыми между собой.

Таким образом, на основе оценок относительной информативности требований к технической основе могут быть сформированы требования к показателям качества ТОСУС, причем с учетом их адаптации при изменении внешних условий функционирования и разработки системы.

Тем самым может быть решена задача определения объема и номенклатуры требований к ПК ТОСУС. Эта задача может и должна быть сформулирована и решена, как задача многокритериального ранжирования по информативности исходной совокупности требований, описывающих ТОСУС при

ограничениях на ресурсы необходимые на реализацию и вероятность достижения требуемой результативности процесса автоматизированного управления связью.

Помимо этого, результаты решения данной задачи, по мнению авторов, позволят повысить адекватность и достоверность описания тех существенных свойств ТОСУС, которые, в целом, и определяют ее качество.

Список используемых источников

1. Башкирцев А. С., Митрофанов Е. А., Паращук И. Б. Анализ требований к автоматизированным системам управления телекоммуникационными сетями // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 8. СПб.: СПОИСУ, 2020. 474 с. С. 91–95.

2. Корлякова М. О., Твердохлеб Н. О. Анализ подходов к определению информативности признаков // Научная сессия МИФИ-2006. Т. 3 Интеллектуальные системы и технологии. М.: МИФИ, 2006. С. 146–147.

3. Федоров В. К., Сергеев Н. П., Кондрашин А. А. Контроль и испытание в проектировании и производстве радиоэлектронных средств. М.: Техносфера, 2005. 563 с.

4. Гаскаров Д. В., Голинкевич Т. А., Мозгалевский А. В. Прогнозирование технического состояния и надежности аппаратуры. М.: Советское радио, 1974. 224 с.

УДК 004.932.4
ГРНТИ 28.23.15

ЭФФЕКТИВНЫЕ ИНСТРУМЕНТЫ ГЕНЕРАЦИИ ИЗОБРАЖЕНИЙ

Е. В. Баягантаева, Т. В. Мусаева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассмотрены существующие продукты для создания картин, их особенности и различия, а также потенциал применения изображений в качестве успешного коммерческого объекта. Использование программ генерации изображений дает возможность не только для творческого выражения человека, но и для использования итоговых изображений для быстрого создания уникальной рекламной продукции, дизайна книжных изданий, одежды и др.

нейронные сети, свёрточные сети, генеративно-состязательные сети, генерация изображений.

Использование нейронных технологий является актуальной областью исследований. В настоящее время нейронные сети активно внедряются во

все сферы жизни человека. Проектирование маршрутов, автопилотирование, распознавание лиц – все это, включая множество других процессов, осуществляется на базе нейронных сетей. Основная их особенность заключается в нахождении неявных зависимостей между входными данными и результатом в обучающей выборке, а также в способности предоставить результат по данным, не входящим в процесс обучения.

Возможность применения нейронных сетей для создания искусства – нетривиальная тема, дающая программистам как свободу в выборе алгоритмов обучения, так и ограничение в виде принадлежности создаваемого к искусству. Разработчики, решая вопрос генерации художественных изображений, реализовали различные инструменты.

Целью настоящей статьи является анализ возможностей существующих программ генерации изображений, которые могут использоваться для решения большого спектра задач в деятельности человека.

Объект исследования – программы генерации изображений, доступные пользователям, не владеющим каким-либо языком программирования, реализованные на Web и мобильной платформах.

Задачи:

1) Поиск приложений.

2) Категорирование приложений.

3) Исследование реализованных инструментов.

4) Выявление особенностей.

5) Определение потенциала использования выходного объекта для коммерческих целей.

Важно отметить, что значение термина «объект искусства» в настоящей статье определяется, как произведение, имитирующее живопись, обладающее законченным характером и самостоятельным художественным значением.

В ходе исследования были найдены следующие продукты: Ostagram, DeepArt.io, Prisma, Vinci, Artisto, DeepArtEffects, ArtBreeder.

Результатом первичного анализа является разделение данных приложений на две категории по принципу их работы:

1. Обработка исходного изображения с целью имитации художественного стиля.

2. Смешивание как минимум двух изображений для генерации нового.

Функционал первой категории инструментов заключается в загрузке пользователем изображения, далее в выборе интересующего его художественного стиля. Работа приложений основана на свёрточных нейронных сетях (CNN) [1]. Используя фильтры, CNN способна распознавать и классифицировать объекты. Пример обработки программы изображен на рис. 1.

Рис. 1. Обработка изображения с помощью программы Painnt

Таблица отражает результаты анализа приложений. Количество скачиваний рассчитывалось по данным GooglePlay, AppStore или из официального сайта продукта (N/A – *not available* – данные отсутствуют в свободном доступе). Выделенные названия указывают на Web платформу инструмента, невыделенные – на мобильную.

ТАБЛИЦА. Результаты анализ приложений первой категории

	Название	Год	Размер изображений	Кол-во стилей	Цена	Кол-во использований
1	Prisma	2016	SD	72	-	120 млн +
			SD/HD	>500	119 руб./мес. 800 руб./год	
2	**Deepart.io**	2015	500×500 px	∞	-	N/A
			HD/ULTRA HD		От 19 до 299 евро за изображение	
3	**Ostagram**	2016	600 px	∞	-	N/A
			HD/ULTRA HD		От 1 до 10 долларов за изображение	
4	Vinci	2016	SD	25	-	1 млн +
			SD/HD	27	69 руб./мес. 599 руб./год	
5	Artisto	2016	720×720px	22	-	1 млн +
6	Deep Art Effects	2016	1080 px	65	-	1 млн +
			HD	123	189 руб.	
			ULTRA HD		69 руб. за изображение	
7	Painnt	2016	700 px/HD	>600	-	10 млн +
			Full HD, 4K, Original size	∞	120 руб./мес. 590 руб./год	

Инструмент Painnt предлагает наиболее выгодное предложение пользователю, предоставляя бесплатно HD качество итогового изображения и более 600 фильтров. Недостатком данного инструмента является отсутствие обновлений с 2017 года [2].

Достоинство Web платформ заключается в возможности применения собственных фильтров. Недостаток – обработка изображений зависит от загруженности сайтов и может достигать десятки минут.

Использование полученных изображений в коммерческих целях возможно только в том случае, если пользователь обладает правами на исходное изображение.

Основной технологией для создания программ второй категории являются генеративно-состязательные сети (сокращённо GAN) [3]. Они состоят из общей работы двух сетей – генератора и дискриминатора. Задача генератора – создать изображения, которые дискриминатор определит, как «подлинные».

Примеры, полученные в результате работы данных программ, представлены на рис. 2.

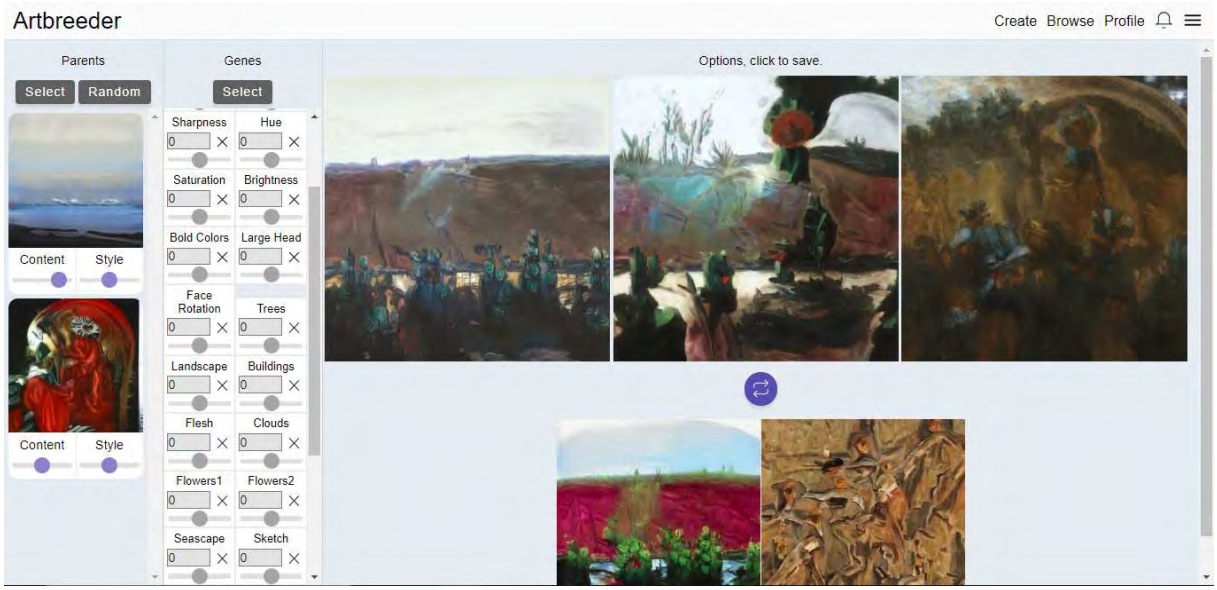


Рис. 2. Смешивание изображений с помощью программы «ArtBreeder»

Ввиду того, что GAN были открыты только в 2014 году, большинство продуктов для генерации изображений ориентировано на пользователей, обладающих навыком программирования. Далее представлен инструмент, попадающий под объект настоящего исследования.

Artbredeer – Web приложение, созданное в 2018 году Джоэлом Сайманом [4]. На данный момент с помощью инструмента были сгенерированы более 54 000 000 изображений. Основная работа программы состоит в выборе изображений, которые пользователь желает смешать для получения

нового. Также являются доступными регуляторы для изменений свойств генерации.

Инструментом можно пользоваться на бесплатном и платном условии. Преимущества платной подписки заключаются в получении изображений высокого качества, увеличении количества изображений для скачивания и загрузки, а также возможности работать конфиденциально. При публикации работы публично другие пользователи могут использовать изображение в качестве исходного для генерации нового продукта, порождая тем самым «сложную родословную» объекта.

Изображения, полученные в результате работы в данной программе, могут быть использованы в коммерческих целях. В случае, когда изображение было создано в результате многочисленных генераций разными участниками, создатель ArtBreeder рассматривает возможность разделения прибыли от продажи полученного объекта между всеми членами процесса его развития [5]. Стоит также отметить, что в данной ситуации, следует проверять «родословную» изображения на наличие в ней веток с нарушением авторских прав.

В настоящее время уже существуют примеры использования нейронных сетей для генерации дизайна коммерческих продуктов. Одним из них является реализация 7 000 000 различных упаковок банок фирмы Nutella в 2017 году, которые были распроданы за один месяц [5]. Проект был выполнен благодаря сотрудничеству фирмы с рекламным агентством Ogilvy&MatherItalia. Данный факт в очередной раз доказывает актуальность и перспективность разработок в области генерации изображений.

Список используемых источников

1. Gatys, L. A.; Ecker, A. S.; Bethge, Matthias. A Neural Algorithm of Artistic Style. URL: https://arxiv.org/pdf/1508.06576.pdf (дата обращения 28.03.2021).

2. Приложение Painnt. URL: https://play.google.com/ store/apps/details?id=io.moonlighting.painnt&hl=ru&gl=US (дата обращения 28.03.2021)

3. Bailey, Jason. The tools of generative art, from flash to neural networks // Art in America: электрон. журн. 2020. URL: https://www.artnews.com/art-in-america/features/generative-art-tools-flash-processing-neural-networks-1202674657/ (дата обращения 28.03.2021).

4. About Artbreeder. URL: https://www.artbreeder.com/about (дата обращения 28.03.2021).

5. Betsy, Mikel. Nutella “Hired” an Algorithm to Design New Jars. And it Was a Sell-Out Success. No two Nutella labels were alike // Inc: электрон. журн. 2017. URL: https://www.inc.com/betsy-mikel/can-robots-do-the-job-of-designers-nutella-gives-it-a-whirl.html (дата обращения 28.03.2021).

УДК 004.7 + 681.5
ГРНТИ 49.37.29

ТЕРРИТОРИАЛЬНЫЙ МОНИТОРИНГ НА ОСНОВЕ АВТОМАТИЧЕСКИХ ПОДВИЖНЫХ СРЕДСТВ СВЯЗИ

С. М. Белов, Л. М. Макаров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Технология ZigBee становятся всё более популярными, за счёт своей универсальной топологии сети, которая даёт большую гибкость при развёртывания локальной сети, а также небольшое энергопотребление своих модулей и вариативность работы в одном диапазоне электромагнитных волн, что в свою очередь предоставляет широкий спектр применений, а развитие робототехники предоставляет возможность объединить эти технологии и занять свою нишу.

технология Zigbee, Wi-fi, Bluetooth, автоматика, роботы.

В настоящее время возрастает потребность в мобильных автоматизированных устройствах, которые будут работать в труднодоступных местах для осуществления мониторинга территорий. На рынке предлагают множества решений, но не каждое из предложенных может удовлетворить клиента. Рассмотрим популярные технологии беспроводных сетей – Wi-fi, Bluetooth и ZigBee.

Рассмотрим существующие технологии, на базе которых можно реализовать мобильные устройства мониторинга.

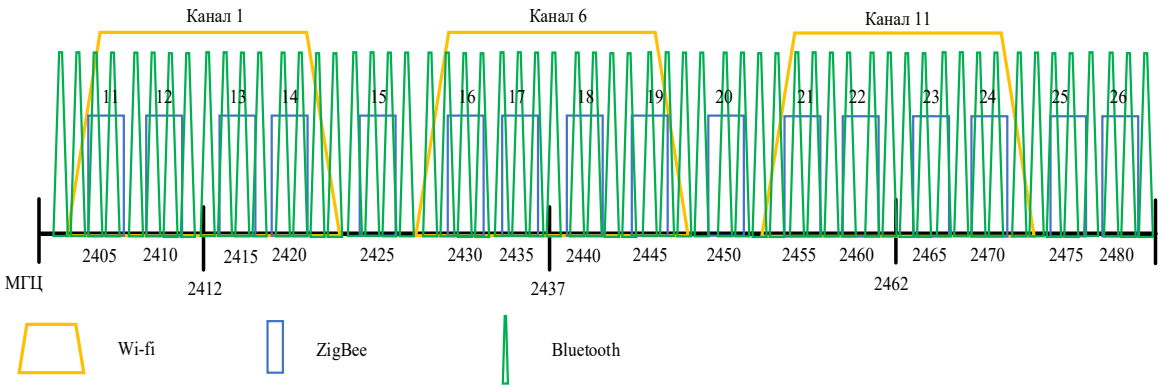


Рис. 1. Спектры электромагнитных волн

Сложно представить в современном обществе человека, который не знает или не пользуется технологией Wi-fi. Данная технология предоставляет широкие возможности по передаче данных по воздуху, таких как скорость и расстояние, которые зависят от стандартов (Рис. 2). Минус такой технологии в том, что устройства энергозатратные, а значит они менее автономны.

Технология Bluetooth (рис. 3), часто использующая для взаимодействия устройств на небольшое расстояние, а также активно применяются для реализации приложений дополненной реальности в рамках концепции города, и в проектах «Умный домой».

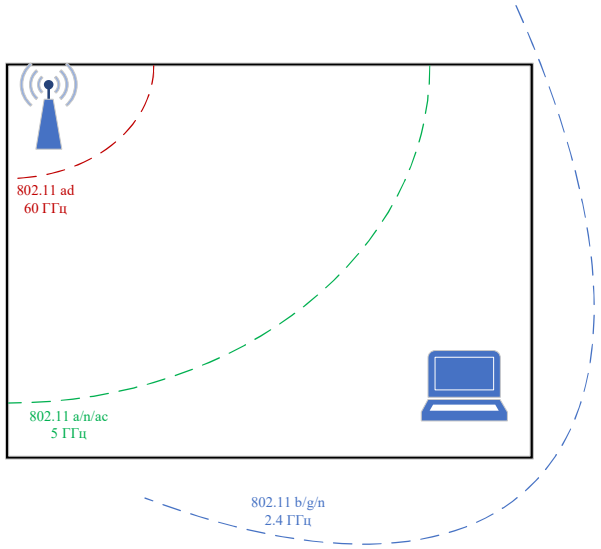


Рис. 2. Зоны покрытия стандартов Wi-fi

Рассмотрим технологию ZigBee, которая в настоящее время применяется для реализации приложений в рамках интернет вещей. Сети ZigBee являются самоорганизующимися сетями и имеют ячеистую топологию, то есть относятся к mesh-сетям. Использование такой топологии, а также специальных алгоритмов маршрутизации позволяет таким сетям быстро восстанавливаться и осуществлять гарантированную доставку пакетов при выходе из строя некоторых узлов. Также спецификация ZigBee реализует гибкую политику безопасности и криптографическую защиту данных. Устройства сети ZigBee небольшого размера, низкой стоимости и с низким потреблением энергии.

Элементами сети ZigBee являются координатор, маршрутизатор и конечные устройства. Спецификация ZigBee предполагает работу сети с различными топологиями. Может быть топология звезда, кластерное дерево, точка-точка и ячеистая (Рис. 4). Наибольший интерес представляет топология ячеистая сети, использующая протоколы динамической маршрутизации, что позволяет создавать самоорганизующиеся и самовосстанавливающиеся сети [1].

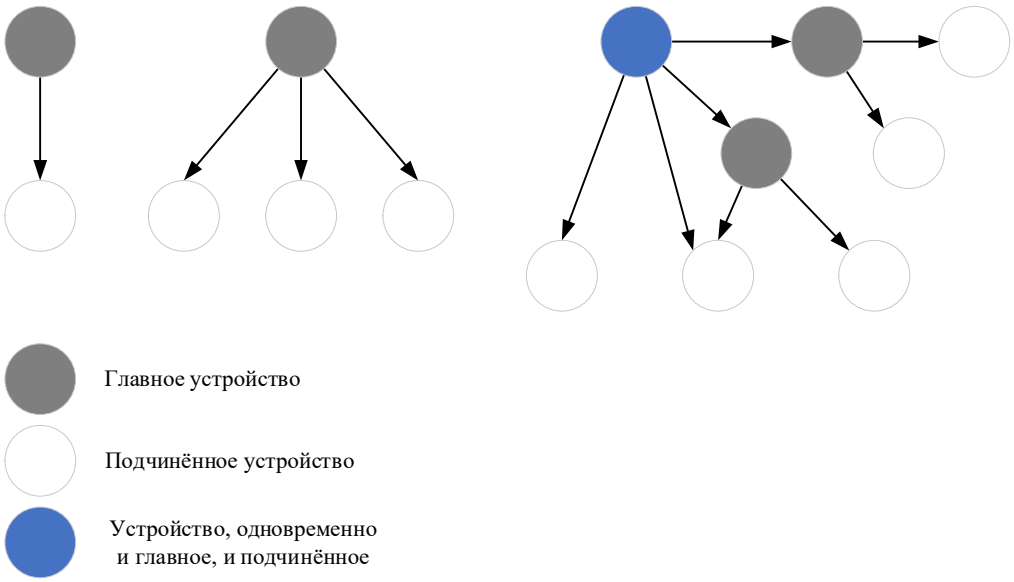


Рис. 3. Структура сети Bluetooth

Из перечисленных ранее беспроводных сетей, можно выбрать как самую подходящею для реализации автоматизированного мониторинга территорий – топологию сети ZigBee. На базе сети ZigBee можно организовать простеющую самоорганизующуюся сеть, представляющую собой огромное количество абонентов на некоторой площади, образующую площадь покрытия сети и несколько точек доступа к внешним сетям. Каждое автоматическая наземная машина (Рис. 5) является абонентом, в зависимости от комплектации обладает своим площадью покрытия и когда находиться в радиусе другого устройства, то он посылает пакеты данных абоненту, находящемуся в центре сети или в любом другом точке доступа, таким образом происходит многоскачковый процесс, где передача пакетов происходит по заранее проложенному маршруту проходя на своём пути через минимально доступное количество узлов, которое в свою очередь образуется от каждого устройства – абонента [2]. Отсюда следует, что каждый абонент может увеличить радиус покрытия сети за счёт своих ресурсов. Следовательно, мощность устройство должна быть минимально необходимое для функционирования поддержания сети, а это позволяет уменьшит стоимость каждого абонента, также увеличить безопасность сети и улучшить электромагнитную совместимость (Рис. 1).

Рассмотрены возможные варианты и подобраны самые подходящие решения, даёт возможность увеличить эффективность обеспечения безопасности разнообразной территории, где человек бессилен перед силой природы, а также улучшает процесс мониторинга территории.

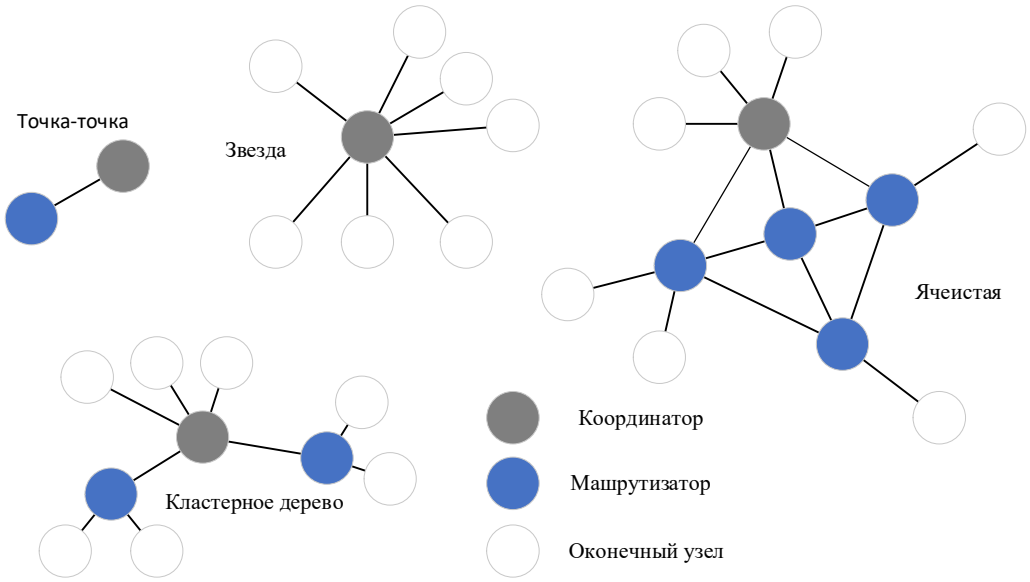


Рис. 4. Примеры топологий сети ZigBee

Рис. 5 Автоматическая наземная машина

Список используемых источников

1. Маколкина М. А. Разработка и исследование комплекса моделей трафика и методов оценки качества для дополненной реальности : дис. … д-ра техн. наук : 05.12.13 / Маколкина Мария Александровна. СПб., 2019. 436 с.

2. Лопота А. В., Николаев А. Б. Наземные робототехнические комплексы военного и специального назначения // Современные тенденции развития робототехнических комплексов: электрон. научн. буклет 30 с. URL: https://rtc.ru/media/images/docs/book/nazemnie.pdf (дата обращения 15.03.2021).

УДК 004.3+007.52+681.34
ГРНТИ 47.14

УЧЕБНЫЙ СТЕНД ДЛЯ ИССЛЕДОВАНИЯ МИКРОКОНТРОЛЛЕРНЫХ ПЛАТ И ЭЛЕКТРОННЫХ МОДУЛЕЙ СИСТЕМ МАЛОЙ АВТОМАТИЗАЦИИ

К. В. Белоус, Е. А. Пиликина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современные системы малой автоматизации в большинстве случаев содержат микроконтроллерную плату с прошивкой, обеспечивающей функционирование устройства по заданному алгоритму, а так же датчики и исполнительные устройства. При их прототипировании одним из важных вопросов является вопрос обеспечения надёжного соединения между компонентами электронных схем.

автоматизация, печатная плата, микроконтроллер, автоматика.

В настоящее время на кафедре Интеллектуальных систем автоматизации и управления сформирована материальная база для исследования и изучения промышленных устройств и компонентов систем управления технологическими процессами и производствами, в то же время стендов, позволяющих исследовать элементы систем малой автоматизации, нет. Имеющиеся в наличии гусеничные роботы на базе микроконтроллеров семейства PIC являются, по большому счёту, законченными комплексами, ориентированными на изучение мобильных робототехнических систем и для исследования разработки устройств малой автоматизации не пригодны [3]. В связи с вышесказанным возникает необходимость создания учебных стендов для исследования систем малой автоматизации.

Традиционный способ создания прототипа устройств – с использованием макетной платы (рис. 1) в данном случае не подходит, так как процесс создания прототипа даже самого простого устройства сопряжён с образованием множества подвижных соединений, что приводит к образованию плавающих соединений, когда в виду особенности коммутации контактов малого диаметра может возникнуть недостаточное сопряжение компонентов проектируемого электронного устройства и всё время, отведённое на исследования схемы, будет потрачено на поиск плавающего соединения.

Выходом из сложившейся ситуации может служить следующе техническое решение: бо́льшая часть компонентов припаивается к печатной плате, а сигнальные выводы компонентов соединяются с коммутационными

гнёздами типа «banana» диаметром 2 мм (рис. 2). Применение гнёзд бо́льшего диаметра не целесообразно, так как это приведёт к увеличению размеров печатных плат, а прочность соединения останется на таком же уровне. Кроме надписей рядом с контактами и компонентами модули так же имеют специальное цветовое оформление коммутационных гнёзд, что практических исключает их ошибочное подключение.

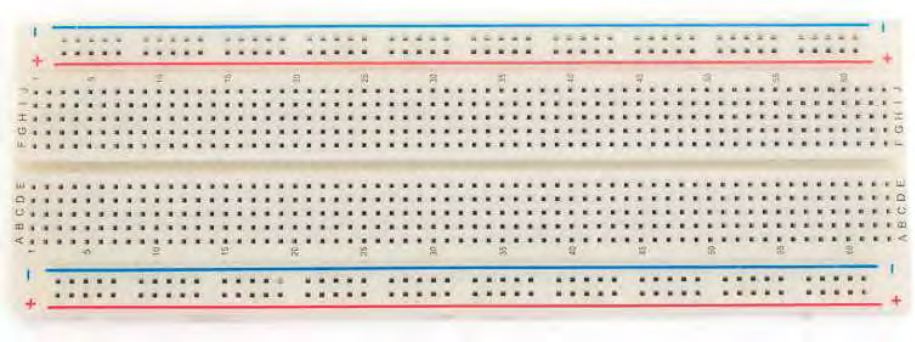


Рис. 1. Классическая макетная плата для прототипирования

При реализации учебных стендов было решено использовать модульный принцип с расчётом на то, что они смогут использоваться и на других дисциплинах. Обобщенная структура стенда представлена на рис. 3. Каждый стендовый модуль содержит определённое количество коннекторов для соединения с другими узлами, при этом их состав и структура могут быть совершенно различными.

Рис. 2. Клеммы типа «Banana»

Все зависимые модули подключаются к главному модулю, содержащему микроконтроллерную плату Arduino Nano, ядром которой является микроконтроллер ATmega328 [2]. В случае если в работе предполагается использовать датчик или компонент, отсутствующие в наборе, можно применить ZIF панель, которая позволяет подключать радиокомпоненты со стандартным шагом между выводами 2,54 мм.

Для подготовки файлов печатной платы, а так же файлов Gerber, которые передаются на производство для создания печатных плат, использовалось программное обеспечение Sprint Layout (рис. 3), позволяющее как создавать многослойные печатные платы, так и проводить тестирование с использованием встроенных средств [1].

Рис. 3. Обобщённая структура стенда

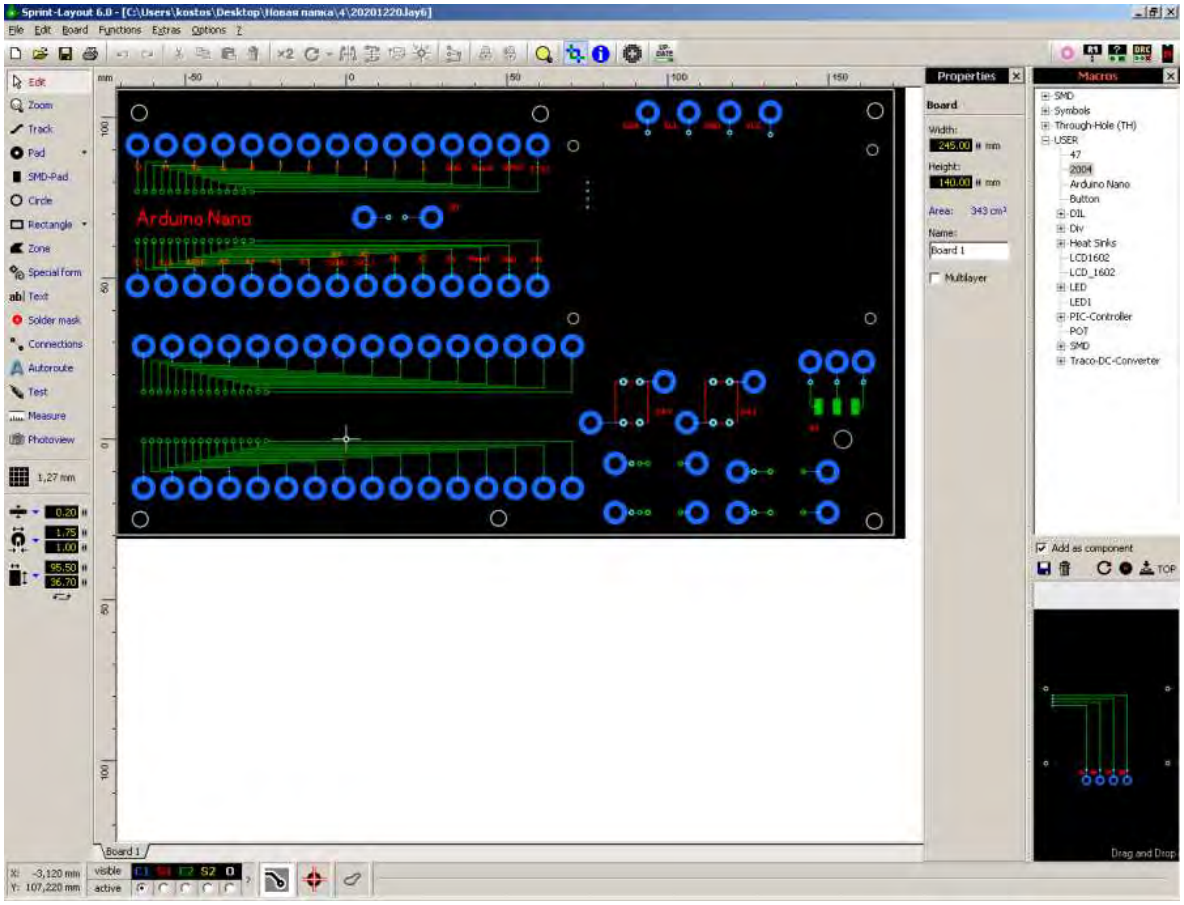


Рис. 4. Задание параметров печатной платы

Для изготовления печатных плат был выбран сервис http://jlcpcb.com, который позволяет выполнить тонкую настройку параметров, если какие-либо данные в исходных Gerber файлах по каким-либо причинам потребуется изменить (рис. 5). Внешний вид печатной платы представлен на рис. 6. Вид готового модуля – на рис. 7.

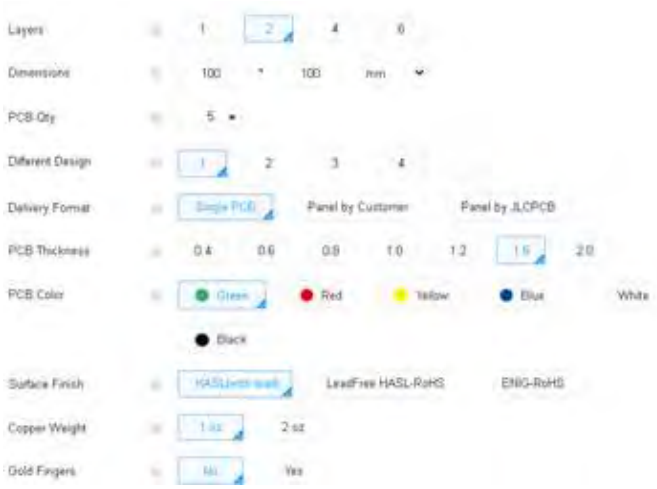


Рис. 56. Обобщённая структура стенда

Рис. 6. Лицевая часть печатной платы

Рис. 7. Оборотная сторона печатной платы

В результате создан модульный учебный стенд, позволяющий экспериментально исследовать различные элементы и устройства систем малой автоматизации, сосредоточившись на изучении электротехнических процессов, протекающих в схемах, а не на подключении и поиске слабо скоммутированного соединения. Представленные учебные модули могут использоваться как самостоятельно, так и в составе более сложных комплексов, таких как, например, NI Elvis.

Список используемых источников

1. Царёв М. Г. Проектирование печатных плат в программе Sprint Layout 6. Ульяновск, 2016. 97 с.: ил.

2. Микушин А. В., Сажнев А. М., Сединин В. И. Цифровые устройства и микропроцессоры: учеб. пособие. СПб.: БХВ-Петербург, 2010. 832 с.: ил.

3. Харрис, Дэвид М. и Харрис, Сара Л. Цифровая схемотехника и архитектура компьютера. 2013. URL: file:///C:/Users/user/Desktop/digital-design-and-computer-architecture-russian-translation.pdf

УДК 004.451.25
ГРНТИ 20.53.01

МЕХАНИЗМЫ УПРАВЛЕНИЯ ПРОЦЕССАМИ В ОПЕРАЦИОННЫХ СИСТЕМАХ ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ ПЛАТФОРМ

И. Б. Бондаренко, Д. И. Мартынов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена изучению принципов работы систем параллельного вычисления многоядерных процессорных устройств. Определяются актуальные операционные системы, рассматриваются механизмы управления и планирования процессами. Принцип работы процессора, работа с самими процессами их циклами в составе масштабируемой системы.

управление процессами, высокопроизводительные платформы, параллельное вычисление.

I. Введение

Различные высокопроизводительные платформы, являются многопроцессорными системами. Такие системы состоят из большого числа серверных компьютеров, соединенных между собой высокоскоростной шиной данных позволяющей достичь максимальной производительности в параллельных вычислениях.

II. Операционная система

Функционирование современных ЭВМ обеспечивается на паритетных началах аппаратными и программными средствами. Программное обеспечение выполняет функцию посредника между пользователями и ЭВМ, расширяет возможности аппаратуры вычислительной машины, являясь логическим ее продолжением [1].

Первые операционные системы адаптировались каждая по отдельности для уникальной разрабатываемой платформы, данное решение было необходимо для увеличения скорости передачи между узлами системы. Со временем тенденция развития операционных систем смещалась от собственных разработок системы к различным вариациям Linux системы, на которых к концу 2017 года работали все высокопроизводительные вычислительные машины из списка TOP500.

Если учесть, что современные используемые решения с массовым параллелизмом как правило отделяют вычисления от других служб, при этом используются различные типы узлов, на вычислительных узлах используется легкое, но более крупная система, по типу «Linux» используется на узлах взаимодействия с пользователем и информацией.

Настройка планировщика задач, а также самой операционной системы в различных конфигурациях является одним из важнейших моментов. Обычно планировщик параллельных заданий состоит из нескольких частей, в которые входит главный планировщик, дающий указания нескольким подчиненным планировщикам на запуск, отслеживание и контроль параллельно выполняемых заданий и периодическое получение от них отчетов о состоянии выполнения заданий.

Несмотря на то, что большая часть используемых на сегодняшний день решений выбирают для работы операционную систему Linux, производители при разработке вносят свои изменения и коррективы в производную системы Linux, которую собираются использовать в дальнейшем. В связи с этим существование отраслевого стандарта невозможно, это обусловлено разнообразием архитектурных решений и специализированных компонентов в системах параллельного вычисления.

III. Планировщик

Планировщик предназначен для решения таких задач как: максимизировать пропускную способность; минимизация времени ожидания; минимизация задержки; времени отклика или обеспечения справедливости. Предпочтение измеряется в зависимости от потребностей и целей пользователя.

Планировщик процессов – это часть операционной системы, которая решает, какой процесс запускается в определенный момент времени. Обычно у него есть возможность приостановить запущенный процесс, переместить его в конец очереди выполнения и запустить новый процесс; такой планировщик известен как планировщик с вытеснением, иначе он является совместным планировщиком [2].

IV. Мультипрограммирование

Процессор за раз способен выполнять одну инструкцию от одной программы, некоторые из этих процессов устойчивы определенный период времени посредством присвоения отдельного процесса к процессору с определенным интервалом, в это время остальные процессы становятся неактивными. Одновременным выполнением при этом считается количество процессов, которые выполняются не единовременно, а в течении определенного периода времени.

Как правило в большинстве компьютерных программах происходит чередование циклов ЦП и ввода-вывода. При выполнении каково либо процесса ЦП выполняет работу для его выполнения, при выполнении цикла ввода-вывода процесс не использует ЦП, в ожидании обработки ввода-вывода.

Для повышения общей производительности вычислительной системы необходимо дать возможность ближайшему в очереди процессу использовать ЦП в тех случаях, когда один из процессов ожидает команды ввода-вывода. При рассмотрении системы с единым программированием, в которой N активных пользователей используют систему для выполнения программ с различным временем на выполнение t_1, t_2, ..., t_N, в которой общее время, t_{uni}, необходимое для того, чтобы обслужить N последовательных процессов для всех N пользователей системы было бы:

$$t_{uni} = t_1 + t_2 + \ldots + t_N.$$

Так как все процессы могут использовать не только циклы ЦП, но и циклы ввода-вывода, количество времени, которое по факту использует ЦП на каждый процесс может составлять лишь малую часть от необходимого времени для выполнения процесса. Для процесса I:

$$t_{i\ (processor)} \ll t_{i\ (execution)},$$

где $t_{i\ (\text{processor})}$ – время, которое процесс затрачивает на использование ЦП;

$t_{i\ (\text{execution})}$– общее время выполнения процесса; т.е. взяв время циклов ЦП и прибавив циклы для ввода-вывода, которые необходимо успеть выполнить до завершения самого процесса. Как правило сумма времени, затраченная процессором на выполнение, используемого N процессами, довольно редко будет превышает малую часть времени, которое необходимо потратить для выполнения любого из выбранных процессов;

$$\sum_{j=1}^{N} t_{j(processor)} < t_{j(execution)}.$$

По этой причине в системах использующих ЦП с единым программированием большую часть времени он может простаивать. Для решения подобных задач с неэффективной работой ЦП используется мультипрограммирование. Подобное решение активно используется в современных ОС, таких как Linux, UNIX и Microsoft Windows. Данное решение дает возможность процессору производить переключение от одного процесса на другой в моменты, когда один из процессов находится в фазе выполнения ввода-

вывода. Так как затрачиваемое время на обработку в разы меньше нежели время необходимое на выполнение одного задания, общее время необходимое для обслуживание всех N активных пользователей сокращается с использованием многопрограммной системы до:

$$t_{\text{multi}} = \max(t_1, t_2, ..., t_N).$$

V. Механизмы управления

Межпроцессное взаимодействие (IPC) – это реализация общего взаимодействия, взаимодействия процессов и потока данных между потоками и/или процессами как внутри узла, так и между узлами. Требования к обмену данными внутри узла и между узлами определяют дизайн низкоуровневого IPC, который является типичным подходом к реализации функций связи, поддерживающих прозрачность. В этом смысле межпроцессное взаимодействие является важнейшей концепцией, лежащей в основе низкоуровневого проектирования распределенной операционной системы [3].

Системные ресурсы распределяются по всей системе на различные узлы системы. Для управления системой необходимо распределять и балансировать используемые ресурсы, для этого необходимо принимать множество решений по типу поиска простаивающих процессов, временем, когда и куда необходимо его переносить. Алгоритмы принятия подобных требует второго уровня политики принятия решений при выборе подходящего алгоритма.

Управление процессами использует политики и механизмы для эффективного разделения ресурсов между узлами и процессами. Они используют различные операции, такие как выделение и отмену распределения процессов и портов процессора, механизмы: остановки, приостановки, миграции, запуска или возобновления выполнения процессов. Подобные операции могут быть локальными или удаленными в отношении друг к другу, ОС должна поддерживать состояние и синхронизацию всех процессов в системе.

Основная обязанность ОС с двумя состояниями контролировать выполнения процессов. Самая простая модель основывается на том, что процессор занимается выполнение процесса либо не занимается. Таким образом процесс находится в одном из двух состояний: РАБОТАЕТ или НЕ РАБОТАЕТ. При создании нового процесса операционной системой, процесс помечается как НЕ РАБОТАЕТ и встает в очередь в состоянии НЕ РАБОТАЕТ. После этого процесс находится в ячейке памяти основного хранилища и встает в очередь до момента вызова на повторное выполнение. После выполнения процесс, ранее помеченный в состоянии как, РАБОТАЕТ прерывается и переводится из состояния РАБОТАЕТ в НЕ РАБОТАЕТ, тем самым освободая

ЦП для следующего в очереди процесса. Диспетчерская часть ОС выбирает из списка ожидающих очереди подходящий для передачи НЕЗАПУЩЕННЫХ. Выбранный ранее процесс из состояния НЕ РАБОТАЕТ переименовывается в состояние РАБОТАЕТ, выполнение данного процесса либо начинается, либо возобновляется, в зависимости от того новый это процесс или запущенный ранее.

Хоть модель, работающая только по двум состояниям очень проста для понимания и доступна для самой ОС отказ от использования третьего состояния ЗАБЛОКИРОВАНО будет означать то, что процессор будет попросту простаивать в моменты переключения процесса с циклов ЦП на циклы для ввода-вывода. В случаях, когда речь идет о управлении процессами высокопроизводительных платформ использование модели по двум состоянии не допустимо. Использование состояния ЗАБЛОКИРОВАНО допустимо для каждого процесса находящегося в ожидании ввода-вывода. В этом случае событие ввода-вывода может означать использование какого-либо устройства или сигнал от другого процесса.

Балансировка нагрузки используется для контроля используемой производительности всех узлов, а также отвечает за переключение между ними в момент разбалансировки системы. Балансировка нагрузки использует функцию выбора процесса для перемещения. Ядро использует различные механизмы выбора, в основном используется выбор на основе приоритета.

Для корректной работы балансира все имеющиеся в системе процессы представлены структурой данных называемые блоком управления процессом «PCB» или дескриптором процесса в Linux. Такие «PCB» содержат в себе всю основную информацию необходимую для работы, а именно:

- Что это?
- Куда это идет?
- Насколько завершена его обработка?
- Где хранится?
- Сколько он «потратил» на использование ресурсов?

VI. Заключение

Дальнейшее исследование будет направлено на углубленное изучение механизмов управления процессами и изучение структуры построения операционных систем высокопроизводительных платформ.

Список используемых источников

1. Партыка Т. Л., Попов И. И. Операционные системы, среды и оболочки : учебное пособие. 2-е изд., испр, и доп. М.: ФОРУМ:ИНФРА-М, 2008. 528 с.

2. Суперкомпьютерные технологии в науке, образовании и промышленности / Под редакцией: академика В. А. Садовничего, академика Г. И. Савина, чл.-корр. РАН Вл. В. Воеводина. М.: Издательство Московского университета, 2009. 232 с.

3. Job Scheduling Strategies for Parallel Processing: by Eitan Frachtenberg and Uwe Schwiegelshohn, 2010. Pp. 138–144. ISBN 3-642-04632-0.

4. Operating System incorporating Windows and UNIX, Colin Ritchie. ISBN 0-8264-6416-5

5. Paul Krzyzanowski (2014-02-19). "Process Scheduling: Who gets to run next?" cs.rutgers.edu. Retrieved 2015-01-11.

УДК 004.056
ГРНТИ 81.93.29

ДЕТЕКТИРОВАНИЕ ФАЛЬСИФИКАЦИИ ГОЛОСА НА ОСНОВЕ СВЕРТОЧНЫХ И РЕКУРРЕНТНЫХ НЕЙРОННЫХ СЕТЕЙ

А. А. Браницкий, Р. И. Марданов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе выполнено исследование моделей глубоких нейронных сетей, применяемых при решении задачи детектирования фальсификации голоса. Для обучения моделей произведена подготовка спектрограмм из голосовых образцов с использованием окна Хэмминга. Проведено обучение моделей на подготовленных спектрограммах при использовании следующих архитектур: только рекуррентных нейронных сетей с использованием долгой краткосрочной памяти (LSTM) или управляемых рекуррентных блоков (GRU), только сверточных нейронных сетей Conv1D (для свертки по оконным спектрам) или Conv2D (для свертки всей спектрограммы) и сочетание обеих архитектур с комбинациями (LSTM+Conv1D, LSTM+Conv2D, GRU+Conv1D, GRU+Conv2D). Приведено сравнение результатов предложенных моделей, что позволяет оценить точность обнаружения фальсификации голоса для каждой модели (архитектуры).

рекуррентные нейронные сети, сверточные нейронные сети, фальсификация голоса.

Предобработка речевых образцов

Для детектирования фальсификации голоса использовались сверточные и рекуррентные нейронные сети, обучающая выборка для которых содержала как обычные образцы человеческой речи (далее human), так и специальным образом преобразованные образцы речи, являющиеся целью детектирования (далее spoof) [1].

Все образцы имели следующие характеристики:

- продолжительность – не более 10,2 секунд;
- частота дискретизации – 16 кГц;
- количество каналов – 1 (моноканал).

Сигналы были преобразованы в спектрограммы с использованием окна Хэмминга, нормализованы по амплитуде со значением от 0 до 1 и приведены до единой длины путем добавления пустых значений, в 634 спектральных окна, что соответствует 10,144 секундам.

Далее образцам была присвоена метка о наличии или отсутствии фальсификации для обучения нейронной сети и проверки результатов на данных для тестирования.

Примеры образцов спектрограмм приведены на рис. 1.

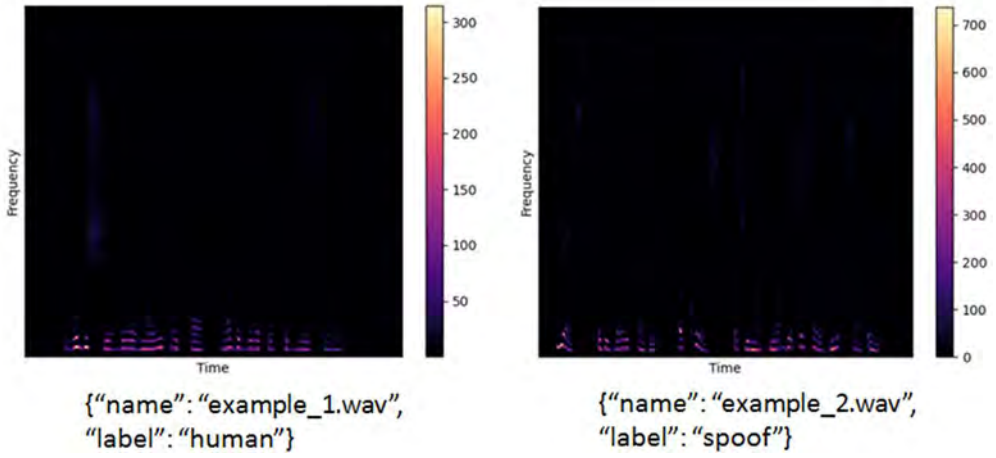


Рис. 1. Образцы спектрограмм

Выбор архитектур.

Для исследования возможности детектирования среди рекуррентных нейронных сетей были выбраны следующие архитектуры:

– сеть долгой краткосрочной памяти (англ. *Long short-term memory*, LSTM) [2];

– управляемые рекуррентные блоки (англ. *Gated Recurrent Units*, GRU) [3].

Среди сверточных нейронных сетей были выбраны следующие архитектуры:

- Conv1D – одномерная свертка спектральных окон.
- Conv2D – двумерная свертка всей спектрограммы.

Параметры при обучении.

Для обучения были взяты 2100 human- и 2100 spoof-образцов речи. Для валидации были взято по 600 образцов для каждого класса, а для тестирования – по 300.

Процесс обучения выполнялся 5 раз, количество эпох обучения – 100.

Результаты обучения

На рис. 2 представлены графики зависимости точности нейронных сетей от номера эпохи на обучающей и валидационной выборках (каждая точка получена в результате усреднения по 5 прогонам).

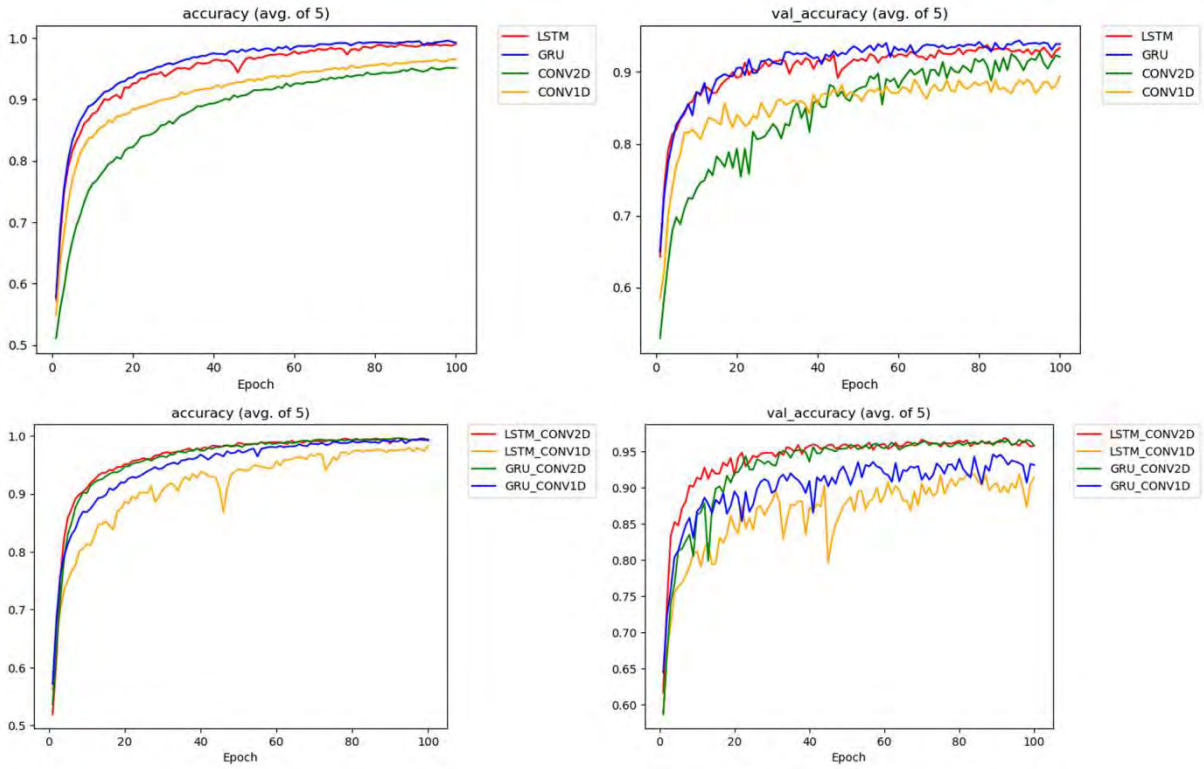


Рис. 2. Графики зависимости точности нейронных сетей от номера эпохи обучения

Оценка качества моделей

Подготовив модель, необходимо адекватно оценить ее качество [4]. Для этого определим следующие понятия:

- TP (True Positive) – истинноположительный прогноз. Реальный класс образца – spoof, спрогнозированный детектором класс – spoof;
- FP (False Positive) – ложноположительный прогноз. Реальный класс образца – human, спрогнозированный детектором класс – spoof. Это так называемые ошибки первого рода. Она не так критична, как ошибка второго рода;
- FN (False Negative) – ложноотрицательный прогноз. Реальный класс образца – spoof, спрогнозированный детектором класс – human. Это так называемые ошибки второго рода. Обычно при создании модели желательно минимизировать число ошибок второго рода, пренебрегая количеством ошибок первого рода;
- TN (True Negative) – истинноотрицательный прогноз. Реальный класс образца – human, спрогнозированный детектором класс – human.

Кроме прямой оценки достоверности в процентах, существуют такие метрики, как точность и полнота, основанные на вышеприведенных результатах бинарной классификации. На основе имеющихся данных выведены метрики качества моделей:

•Метрика достоверности (англ. *Accuracy*) (показывает общее количество верных предсказаний):

$$Accuracy = (TP+TN)/(TP+FP+FN+TN);$$

•Точность (англ. *precision*) (показывает отношение верно распознанных объектов класса ко всем объектам, которые определены как объекты класса):

$$Precision = TP/(TP+FP);$$

•Полнота (англ. *recall*) (показывает отношение верно распознанных объектов класса ко всем представителям этого класса):

$$Recall = TP/(TP+FN);$$

•F-мера (англ. F1-*score*) (среднее гармоническое точности и полноты, помогает сравнить модели, используя одну числовую меру):

$$F1 = 2 \cdot Precision \cdot Recall/(Precision+Recall).$$

Используя все эти метрики, выполним оценку моделей на отдельной проверочной выборке в 6 000 образцов речи, не участвовавших при обучении моделей. Результаты оценки приведены в таблицах 1 и 2.

ТАБЛИЦА 1. Таблица контингентности

Модель	**TP**	**FP**	**FN**	**TN**
LSTM	2830	158	170	2842
GRU	2820	203	180	2797
Conv2D	2597	82	403	2918
Conv1D	2639	405	361	2595
LSTM+Conv2D	2905	59	95	2941
LSTM+Conv1D	2676	83	324	2917
GRU+Conv2D	2908	78	92	2922
GRU+Conv1D	2603	65	397	2935

ТАБЛИЦА 2. Таблица оценки моделей

Модель	Accuracy, %	Precision, %	Recall, %	F1 score, %
LSTM	94,53	94,71	94,33	94,52
GRU	93,62	93,28	94,00	93,64
Conv2D	91,92	96,94	86,57	91,45
Conv1D	87,23	86,69	87,97	87,33
LSTM+Conv2D	**97,43**	**98,01**	**96,83**	**97,42**
LSTM+Conv1D	93,22	96,99	89,20	92,93
GRU+Conv2D	**97,17**	**97,39**	**96,93**	**97,16**
GRU+Conv1D	92,30	97,56	86,77	91,85

Как видно из табл. 2, самый лучший результат показали модели LSTM+Conv2D и GRU+Conv2D со средними значениями достоверности и F-меры более 97 %.

Заключение

По итогам обучения и тестирования лучшие результаты показали обе архитектуры рекуррентных нейронных сетей с совместным использованием двумерной свертки спектрограмм.

Список используемых источников

1. Марданов Р. И. Методика обнаружения фальсификации сигнала речи в биометрических системах аутентификации с использованием глубокой нейронной сети // Подготовка профессиональных кадров в магистратуре для цифровой экономики : материалы региональной научно-технической конференции магистров и их руководителей, СПб., 1–3 дек. 2020 г. СПб.: СПбГУТ, 2020. С. 427–431. URL: http://pkm.sut.ru/documents/materials_2020.pdf (дата обращения 25.02.2020).

2. LSTM – сети долгой краткосрочной памяти. URL: https://habr.com/ru/company/wunderfund/blog/331310/ (дата обращения 25.02.2021).

3. Gate-variants of Gated Recurrent Unit (GRU) neural networks. URL: https://ieeexplore.ieee.org/document/8053243 (дата обращения 25.02.2021).

4. Краткий курс машинного обучения или как создать нейронную сеть для решения скоринг задачи. URL: https://habr.com/ru/post/340792/ (дата обращения 25.02.2021).

УДК 66.012.37
ГРНТИ 20.19.17

ПОТРЕБЛЕНИЕ ЭЛЕКТРОЭНЕРГИИ В УСЛОВИЯХ ПАНДЕМИИ COVID-19: CASE STUDY

Е. В. Бунякина[1], **М. И. Гальченко**[2], **А. Г. Гущинский**[3]

[1]ВУНЦ ВМФ «Военно-морская академия»
[2]Санкт-Петербургский государственный аграрный университет
[3]Учебный комплекс ПАО «Россети Ленэнерго»

Анализ и прогнозирование временных рядов отображает резкие изменения окружения, которые могут приводить к слому тенденций временного ряда. Последние события, связанные с карантином по COVID-19, ставят новый вопрос: насколько принятые решения по изоляции граждан и изменению режима работы предприятий меняют шаблоны потребления электроэнергии.

COVID-19 пандемия, данные, временные ряды, энергия, электроэнергия.

Материалы и методы

Для исследования были загружены данные о входящей мощности (*greed feed-in*) в зоне ответственности компании 50Hertz Transmission GmbH (ФРГ, https://www.50hertz.com/) (рис. 1).

Согласно определению, данному на сайте компании «Энергия, переданная в сеть – это сумма всей мощности, подаваемой от хабов, генерирующих единиц и распределительных сетей в сеть передачи электроэнергии». Таким образом, можно считать, что данные показывают отпуск электроэнергии конечным потребителям. Для анализа были загружены данные от 2015-01-01 до 2020-08-06 с сайта компании. Данные приводятся с шагом в 15 минут.

Рис. 1. Зона ответственности 50Hertz Transmission GmbH (источник – сайт компании)

Обработка проводилась с применением языка статистического программирования *R* [1]. Для оценки статистической значимости различий применяли критерий Манна-Уитни-Уилкоксона, для оценки различий

в шаблонах потребления применяли периодограмму Ломба-Скаргла (*Lomb-Scargle*), расстояние между рядами вычисляли с помощью DTW и расстояния Фурье. Также была использована библиотека prophet для получения разложения ряда на тренд и сезонные составляющие.

Обсуждение

Согласно приводимой истории введения коронавирусных ограничений в Германии [2] можно выделить следующие даты:

1. 27 января – первый случай заражения.
2. 10 марта – запрет на проведение мероприятий с количеством участников более 1 000 человек.
3. 14 марта – ограничения в работе школ, ресторанов и прочих организаций (в зависимости от земли).
4. 16 марта – закрытие границ.
5. 19–22 марта – введение социальной дистанции, ужесточение ограничений.
6. 15 апреля – 11 мая первичное снятие ограничений.

Таким образом, интересующий период времени охватывает март-июнь. Для обеспечения полного охвата недель были отобраны недели года с 9 по 27. Суммарная мощность в разрезе по неделям в 2020 году оказалась меньше, нежели во все предыдущие годы в рамках анализируемого периода (рис. 2).

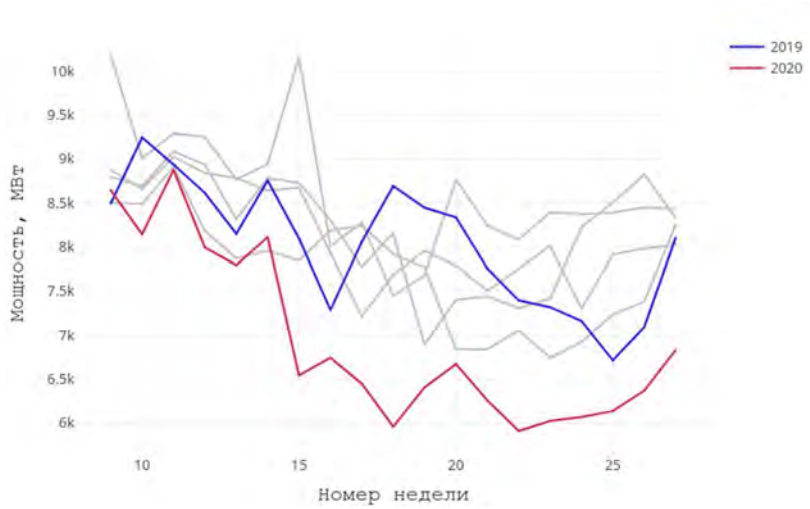


Рис. 2. Суммарная мощность с 9 по 27 неделю.
Серым цветом показаны данные за предыдущие годы

Также можно отметить нехарактерно резкий спад в потреблении электроэнергии на 14–15 неделе (конец марта – начало апреля, наиболее сильные карантинные ограничения). Обращает на себя внимание тот факт, что исторические данные находятся выше по всему анализируемому периоду,

что позволяет сформулировать гипотезу о систематическом превышении результатов прогнозов по моделям, учитывавшим исключительно исторические и погодные данные относительно реальных уровней потребления.

Аналогичная ситуация наблюдается и при анализе данных за выбранные недели. Если рассматривать данные за два последних (2019 и 2020) года, можно отметить, что разброс значений практически идентичен, однако изменились сами формы распределений, медианы в 2020 году смещены относительно 2019 вниз по всем дням недели, за исключением воскресенья (рис. 3).

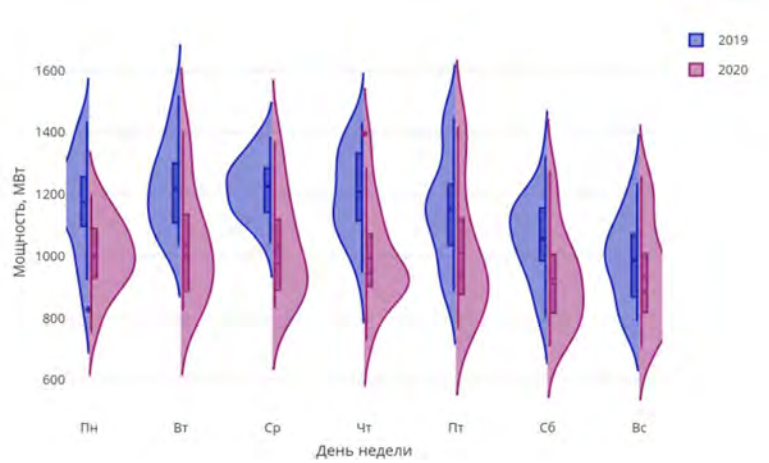


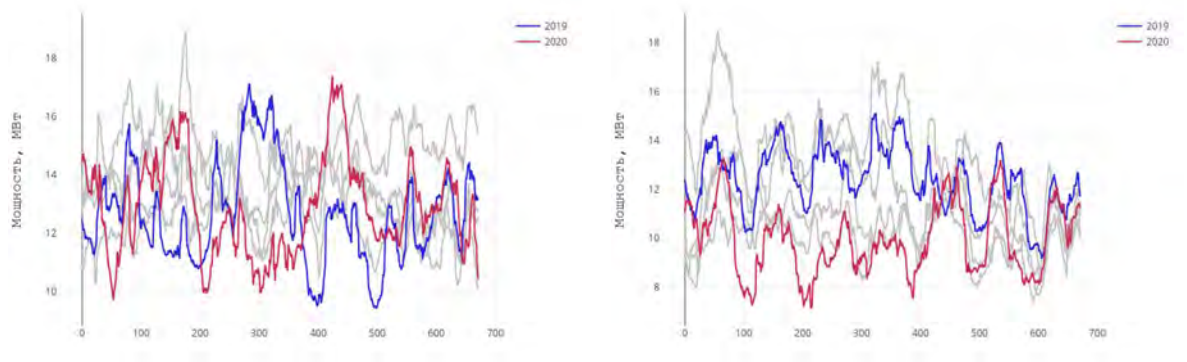
Рис. 3. Распределение мощности по дням недели, 2019 и 2020 год, 9–27 неделя

Для более полной оценки распределений были рассчитаны медианы, их 95 % доверительные интервалы, и интервал первая квартиль – третья квартиль, а также выполне тест Манна-Уитни-Уилкоксона (табл. 1).

ТАБЛИЦА 1. Характеристики распределений по дням недели, 9–27 неделя

День недели	**2019**		**2020**		**p-value**
	Медиана (95 % ДИ)	**[Q1, Q3]**	**Медиана (95 % ДИ)**	**[Q1, Q3]**	
Понедельник	1 170, [1 140, 1240]	[1 111, 1 251]	996, [948, 1 080]	[937, 1 085]	0,0006
Вторник	1220, [1130, 1300]	[1 114, 1 300]	1010, [905, 1 100]	[895, 1 125]	0,0008
Среда	1230, [1 150, 1280]	[1 146, 1 284]	977, [901, 1 110]	[895, 1 115]	0,0002
Четверг	1210, [1 110, 1310]	[1114, 1 324]	948, [910, 1 070]	[906, 1 070]	0,0002
Пятница	1150, [1 090, 1 220]	[1055, 1228]	934, [884, 1 100]	[879, 1 115]	0,01
Суббота	1050, [1 000, 1 150]	[992, 1 154]	915, [822, 998]	[820, 1 004]	0,005
Воскресенье	991, [897, 1 050]	[879, 1 065]	888, [834, 989]	[824, 1 002]	0,26

Таким образом, наблюдается снижение потребления по всем дням недели, снижение статистически значимо за исключением воскресных дней, что показывают и недельные графики (рис. 4), на которых достаточно хорошо видны последствия ограничений от достаточно высокого уровня соответствия данных 2019 и 2020 года за девятую неделю (нормализованное расстояние dtw = 2,53) до значительного снижения объёмов потребления в будние дни двадцатой недели (нормализованное расстояние dtw = 5,55). Вообще говоря, можно отметить сглаживание колебаний в течении недели в 2020 году относительно 2019 года, что может говорить о менее выраженном недельном ритме, за исключением спада потребления в субботу и воскресенье.



(a) (b)

Рис. 4. Мощность, график мощности в сети, исходные данные, на 9 неделю (a) и 22 неделю (b)

Для оценки различий между временными рядами в исследуемый промежуток времени используем расстояние Фурье [5], которое позволяет оценить различия между структурой рядов с помощью коэффициентов, получаемых в результате быстрого преобразования Фурье (FFT). Была построена матрица различий расстояний, значения нормированы по максимальному в столбце (табл. 2).

ТАБЛИЦА 2. Расстояние Фурье, 9–27 неделя

Год/Год	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**
2015	0,00	0,92	0,91	0,93	0,95	0,97
2016	0,87	0,00	0,86	0,90	0,92	0,92
2017	0,88	0,87	0,00	0,92	0,93	0,94
2018	0,96	0,97	0,98	0,00	0,99	1,00
2019	0,96	0,97	0,97	0,97	0,00	0,98

Год/Год	2015	2016	2017	2018	2019	2020
2020	1,00	1,00	1,00	1,00	1,00	0,00

Можно уверенно говорить о том, что по частотной составляющей ряды близки друг к другу, но, при этом максимальные значения расстояния Фурье соответствуют 2020 году, что подтверждает вывод о качественных изменениях в структуре ряда.

Заметно резкое снижение значений в дневном тренде, начиная с середины апреля до конца периода. Колебания в течении недели сглажены, не превосходят, в основном 0,5 МВт по модулю. Фактически, кроме некоторого повышения в среду и спада в воскресенье ритм по дням недели не сохранился относительно 2019 года, где изменения были более существенны. Дневной ритм стал более выраженным: резкий спад потребления в ночное время, утренние часы, подъём потребления в дневные часы и спад в вечерние, что полностью согласуется с предыдущими выводами.

Выводы

В данном случае можно говорить о наличии изменения электроэнергии как в количественном выражении, так и в структуре потребления. Пандемия COVID-19 внесла существенные изменения в характеристики потребление электрической энергии (логично предположить, что «промышленное» потребление упало, а «бытовое» увеличилось, имеется связь с экономическими показателями).

Список используемых источников

1. R Core Team R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. URL: https://www.R-project.org/ (дата обращения 06.08.2020).

2. Lothar Wieler, Ute Rexroth, René Gottschalk Emerging COVID-19 success story: Germany’s strong enabling environment // Our World in Data, URL: https://ourworldindata.org/covid-exemplar-germany (дата обращения 06.08.2020)

3. Ruf, T. The Lomb-Scargle Periodogram in Biological Rhythm Research: Analysis of Incomplete and Unequally Spaced Time-Series // Biological Rhythm Research. 1999. 30:2. Pp. 178–201. doi: 10.1076/brhm.30.2.178.1422

4. Balzer, Paul Was macht der FFT Algorithmus? // URL: https://www.cbcity.de/die-fft-mit-python-einfach-erklaert, (дата обращения 06.08.2020)

5. Mori, Usue, Mendiburu, Alexander, Lozano, Jose Distance Measures for Time Series in R: The TSdist Package // The R Journal. 2016. № 8. doi: 10.32614/RJ-2016-058.

6. Taylor, Sean J., Letham, Benjamin Forecasting at scale // The American Statistician. 2018. Vol. 72, 1. Pp. 37–45.

Статья представлена заведующим кафедрой Информационных технологий ВУНЦ ВМФ «Военно-морская академия» кандидатом технических наук, профессором В. Г. Каревым.

УДК 621.317
ГРНТИ 45.01.85

РАЗРАБОТКА МЕТОДА ПРОЕКТИРОВАНИЯ СИСТЕМЫ ПЕРВИЧНОЙ ОБРАБОТКИ СИГНАЛА

А. В. Ваганов, А. С. Иванов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются вопросы, связанные с разработкой метода проектирования тракта предварительной обработки сигнала от первичных измерительных преобразователей (датчиков) для применения в различных системах автоматизированного управления. Производится синтез структуры и описание блоков, входящих в систему предварительной обработки. Обоснован выбор современной элементной базы для разработки тракта на основе дискретно-аналоговых динамически программируемых электронных систем. Обоснован выбор математического аппарата для создания и исследования моделей блоков тракта предварительной обработки. Произведен выбор математического пакета для реализации аналитического исследования полученных моделей блоков тракта предварительной обработки сигнала. Приведены результаты моделирования и осуществлен их анализ.

дискретно-аналоговые схемы, синтез, анализ, тракт обработки, структура.

Средства предварительной обработки предназначены для обработки исходных сигналов, наблюдаемых в общем случае на фоне случайных шумов и помех различной физической природы и представленных в виде дискретных цифровых отсчетов, с целью обнаружения и выделения полезного сигнала, его пеленгования и оценки характеристик обнаруженного сигнала.

Классическая реализация тракта предварительной обработки сигнала базируется на традиционных дискретных аналоговых элементах: операционные усилители, транзисторы, резисторы, конденсаторы, компараторы и др. Такая реализация имеет следующие недостатки: большие массо-габаритные показатели, отсутствие возможности динамического изменения конфигурации схемы, высокая погрешность и низкая температурно-временная стабильность.

Постепенно по мере снижения стоимости вычислительных систем, аналоговая обработка сигналов вытеснялась цифровой, которая предоставляет возможность практически полностью исключить искажения сигнала при его передаче. Однако, и сейчас имеются определенные области применения аналоговой обработки в различных системах сбора данных и управления. Многие устройства, датчики остаются сугубо аналоговыми и зачастую работают в более тяжёлых условиях эксплуатации и требуют предварительной обработки сигнала. Характерная особенность аналогового датчика – малая

величина амплитуды полезного сигнала, наличие статической помехи в виде постоянной составляющей сигнала, а также влияние на него различных помех от внешних источников.

Однако, не стоит забывать, что тракт первичной обработки сигналов с аналоговым датчиком уязвим к помехам. Обычно для минимизации помех в трактах обработки сигнала эффективны следующие мероприятия: экранирование сигнального, межблочное экранирование, применение различных фильтров (полосовые, режекторные), правильное размещение самих блоков друг относительно друга внутри корпуса прибора [1].

В современной обработке сигнала применяются различные дискретно-аналоговые системы, которые были описаны в предыдущей работе [2]. В отличие от цифровых систем, где сигнал дискретен по времени и квантован по уровню, в аналоговых системах сигнал дискретен только по времени, в силу этого выходной аналоговый сигнал можно восстановить без искажений по его выборкам и точность преобразования может достигать десятых долей процента.

Задача тракта предварительной обработки сигнала – это повышение соотношения сигнал-шум, а значит максимизация энергии полезного сигнала. Данная задача решается комплексно с использованием, в том числе, полосовой фильтрации сигнала. Для ряда задач (регуляторы в системах управления) устройства аналоговой обработки могут оказаться надёжнее сопоставимых устройств цифровой обработки. Всё это означает, что в специализированных областях применения аналоговая обработка сигнала остаётся по-прежнему актуальной [3].

Структурная схема тракта предварительной обработки сигнала от аналогового измерительного преобразователя, являющегося основой обнаружителя полезного сигнала на фоне различных помех, представлена на рис. 1.

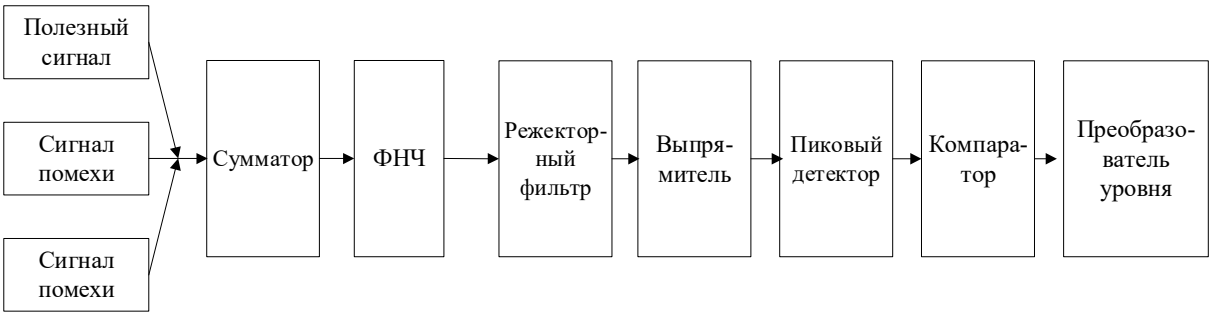


Рис. 1. Блок-схема обнаружителя

Разрабатываемая система содержит следующие элементы: источники полезного сигнала и помех, сумматор, ФНЧ, режекторный фильтр, выпрямитель, пиковый детектор, компаратор, преобразователь уровня.

1) Блоки полезного сигнала.

Данные блоки имитируют измерительный преобразователь и состоят из генераторов синусоидальных сигналов. На выходе блока формируется сигнал с заданной амплитудой и частотой соответствующий реальному.

2) Блок сигнала помехи.

Данный блок имитируется генератором синусоидального сигнала, на выходе которого имеется сигнал помехи.

3) Сумматор.

На вход сумматора подается три напряжения: напряжение полезного сигнала U_{c1} и напряжения помех – $U_{\text{п}1}$, $U_{\text{п}2}$. На выходе сумматора получаем полезный сигнал с помехой.

4) Режекторный фильтр.

Данный блок предназначен для удаления из полосы полезного сигнала помехи. Режекторный фильтр минимизирует влияние сигнала в узком диапазоне заданной центральной частоты (f_0), сигналы выше или ниже узкой полосы ($f_0 \pm \Delta f$), заграждения пропускаются.

5) Выпрямитель.

В устройстве используется двухполупериодный выпрямитель. Это устройство преобразования переменного напряжения в постоянное, работающее по принципу бесконтактной коммутации используемых выводов источника переменного напряжения с нагрузкой, создавая однополярное питание.

6) Пиковый детектор.

Устройство для получения огибающей сигнала, представляющее собой последовательное соединение диода и конденсатора. Данный блок оптимизирует работу компаратора, которому нужно время на переключение.

7) Компаратор.

Пороговое устройство сравнивает значения входного сигнала с опорным и формирует единицу, если входной сигнал больше опорного и ноль – если наоборот. Данный блок необходим, для индикации наличия или отсутствие информативной составляющей во входном сигнале.

8) Преобразователь уровня.

Данное устройство предназначено для обеспечения заданного сигнала на выходе устройства, которое равно одному из двух значений напряжения при наличии или отсутствии сигнала соответственно.

Для удобства описания дискретно-аналоговых устройств используют аппарат для цифровых систем – z-преобразование. Но если частота дискретизации в 100 раз больше максимальной частоты полезного сигнала, то для описания подобных систем можно использовать аппарат передаточных функций, полученных с применением преобразования Лапласа [4].

Применение данного аппарата обусловлено простотой решения линейных дифференциальных уравнений, которые, в свою очередь описывают работу аналоговых устройств. Исследование свойств аналоговых цепей, в частности определение устойчивости, удобно проводить на основе обобщенной передаточной функции всего тракта.

В ходе разработки методики, в качестве примера, произведен анализ фильтра нижних частот, который формируется внутри чипов AN220E04 и AN221E04. Принципиальная схема ФНЧ представлена на рис. 2.

Передаточная функция для этой схемы можно записать в следующем виде (1):

$$\frac{V_{out}(s)}{V_{in}(s)} = \frac{\pm 4\pi^2 {f_0}^2 G}{S^2 + \frac{2\pi f_0}{Q} s + 4\pi^2 {f_0}^2} \quad (1)$$

где G – коэффициент усиления в полосе пропускания (усиление по постоянному току),

f_0 – угловая частота,

Q – добротность.

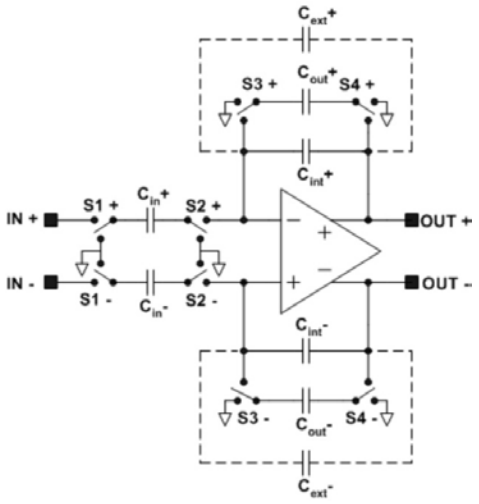


Рис. 2. Схема ФНЧ

Для моделирования тракта предварительной обработки сигнала существует множество математических пакетов. Наиболее предпочтительными являются MathCAD и Matlab. Благодаря удобному интерфейсу, позволяющему записывать математические выражения в символьном виде, для осуществления аналитического исследования тракта обработки была выбрана САПР MathCAD [5].

Данная программа ориентирована, преимущественно на специалистов-разработчиков. MathCAD также используется в сложных проектах, чтобы визуализировать результаты математического моделирования путём использования традиционных языков программирования. Также, MathCAD используется в крупных инженерных проектах, где большое значение имеет трассируемость и соответствие стандартам.

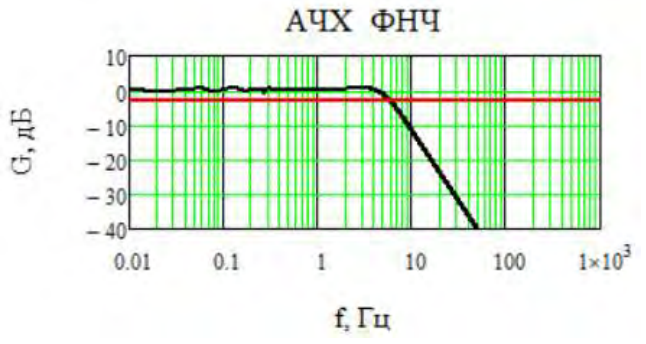


Рис. 3. АЧХ фильтра нижних частот

Результат работы программы построения АЧХ фильтра нижних частот на 5 Гц в САПР MathCAD показан на рис. 3.

В заключении следует отметить, что использование дискретно-аналоговых устройств в современных разработках для различных областей, включая и системы управления, является актуальным. Для построения и описания моделей устройств подобного класса можно использовать традиционный математический аппарат передаточных функций в z-области. Моделирование тракта первичной обработки сигнала в САПР MathCAD позволяет проводить эффективный анализ системы.

Список используемых источников

1. Полищук А. Программируемые аналоговые ИС Anadigm структура и принцип построения // Современная электроника. 2005. № 1. С. 84–87.

2. Ваганов А. В., Иванов А. С. Тракт первичной обработки сигнала, как элемент системы сбора данных в АСУ // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПБГУТ, 2020. Т. 2. С. 136–141.

3. Щерба А. М. Программируемые аналоговые схемы Anadigm. использование виртуальных генераторов сигналов в САПР Anadigmdesigner // Компоненты и технологии. 2015. № 12. С. 6–8.

4. Волович Г. И. Схемотехника аналоговых и аналогово-цифровых электронных устройств. М.: Додэка-XXI, 2011. 528 с. ISBN 978-5-94120-254-6.

5. Полищук А., Полищук А. Система автоматизированного проектирования программируемых аналоговых интегральных схем AnadigmDesigner 2. URL: https://kit-e.ru/fpga/sistema-avtomatizirovannogo-proektirovaniya-programmiruemyh-analogovyh-integralnyh-shem-anadigmdesigner-2-chast-1-1-znakomstvo-s-interfejsom (дата обращения 14.02.2021).

Статья представлена заведующей кафедрой ИСАУ СПбГУТ, доктором технических наук, профессором Г. В. Верховой.

УДК 621.317
ГРНТИ 45.01.85

РАЗРАБОТКА МЕТОДА ПРОЕКТИРОВАНИЯ СИСТЕМЫ ПИТАНИЯ В АСУ

А. В. Ваганов, С. С. Серегин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются вопросы, связанные с разработкой метода проектирования систем электропитания (СЭП) современных комплексов автоматизированного управления предприятий. Производится синтез структуры и описание блоков, входящих

в систему электропитания. Обоснован выбор современной элементной базы для разработки СЭП. Обоснован выбор математического аппарата для создания и исследования моделей отдельных блоков системы электропитания. Произведен выбор математического пакета для реализации аналитического исследования полученных моделей блоков СЭП для автоматизированных систем управления. Приведены результаты моделирования и осуществлен их анализ.

СЭП, АСУ, автоматизация, электроснабжение, распределение энергии.

В настоящее время системы автоматизированного управления (АСУ) находят все более широкое применение в современном производстве. Основной целью применения и использования АСУ выступает повышение эффективности использования каждого объекта производства. Данные системы позволяют быстро и эффективно проводить анализ работы объекта, а на основе полученных данных специалисты могут принять определенные решения и наладить производственный процесс. Различают автоматизированные системы управления объектами (технологическими процессами – АСУТП, предприятием – АСУП, отраслью – ОАСУ) и функциональные автоматизированные системы, например, проектирование плановых расчётов, материально-технического снабжения и т. д.

В основе управления АСУТП лежат сложные многоуровневые электронные системы, которые требуют надежного и бесперебойного, электроснабжения. Возникающие в сети помехи от коммутации мощного оборудования или резкое изменение напряжения сети (обрыв линии или попадание в нее молнии) могут нарушить правильную работу или привести к повреждению дорогостоящего оборудования АСУ. Выходом из данной ситуации является внедрение специализированных систем электропитания (СЭП). Над решением подобных задач трудятся специалисты различных всемирно известных фирм, например таких как: Siemens, Emerson Electric Company, Cisco и др.

Предлагаемые данными фирмами решения позволяют организовать бесперебойное питание АСУ и обладают следующими преимуществами и недостатками.

В качестве преимуществ следует отметить следующее: высокую надежность, мощную нагрузочную способность, наличие автономного источника электрической энергии, возможность коммутации (отключения) от первичной сети, микропрограммное управление.

К недостаткам отнесем: относительно высокую стоимость, сложность в обслуживании и ремонте, малую универсальность, ограниченную адаптацию к изменяющимся внешним условиям, ограниченную обратную связь с конечным пользователем.

В связи с вышесказанным актуальность разработки метода проектирования и исследования новой СЭП для АСУ продиктована необходимостью

минимизации указанных недостатков с сохранением существующих преимуществ.

С учетом необходимых требований была синтезирована структурная схема разрабатываемой СЭП, показанная на рис. 1. Одной из отличительных особенностей новой системы электропитания является ее адаптивность, которая заключается, в том числе, и в возможности подстройки системы к изменяющимся условиям внешней среды (повышение температуры или влажности, повышенная вибрация и т. п.). Благодаря наличию данной особенности и применению микропроцессорного управления новой СЭП появляется возможность предугадывать появление аварийных ситуаций (пожар, землетрясение и т. д.) для выработки упреждающих защитных мер для предотвращения поврежденияоборудования АСУ и человеческих жертв (поражение электрическим током от поврежденного оборудования).

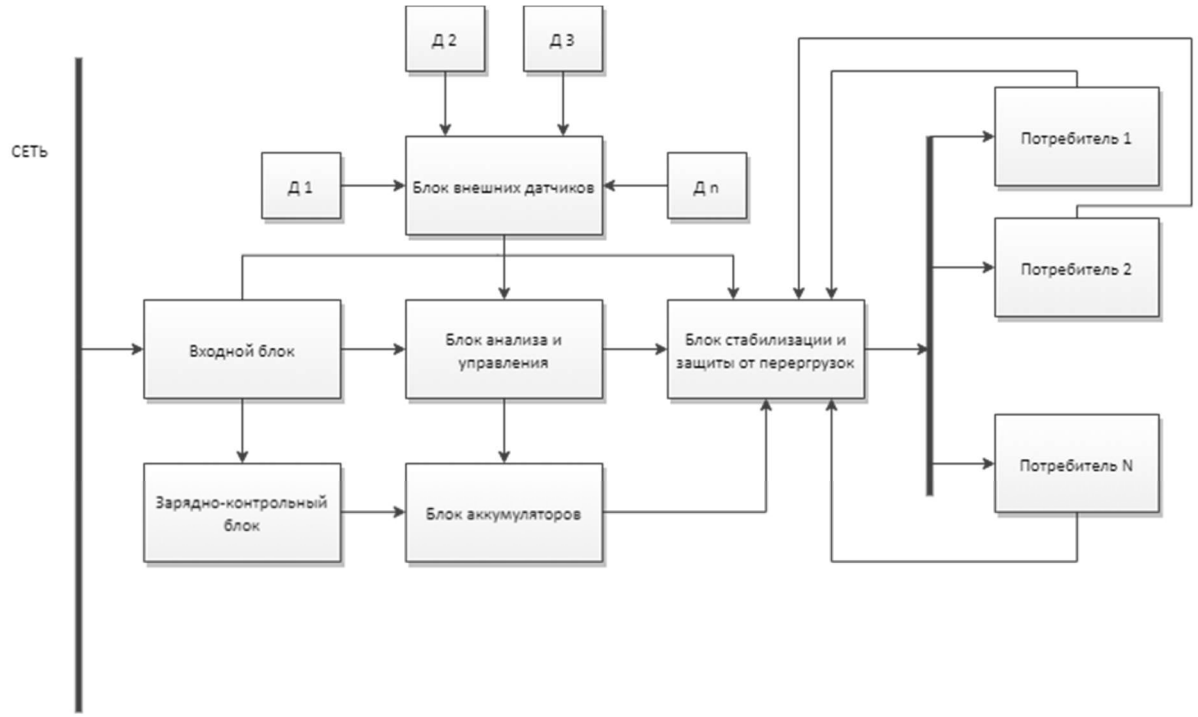


Рис. 1. Новая структурная схема СЭП

В качестве сенсоров новой СЭП выступают различные датчики физических параметров, обозначенные на структуре как Д1-Дn. В ходе сборки и отладки системы эти датчики могут изменяться пользователем в зависимости от расположения СЭП и решаемых ею задач.

При разработке метода также важным является выбор математического аппарата и разработка математических моделей каждого блока. Для примера был рассмотрен фрагмент входного блока, представляющий собой сетевой фильтр высокочастотных помех. Схема данного фильтра представлена на рис. 2.

Основной задачей такого фильтра является снижение амплитуды сигналов помех, возникающих в электросети, и лежащих в частотной полосе выше нескольких килогерц. Токовый ключ (SC) обеспечивает защиту подключенных потребителей от перегрузок и токов коротких замыканий. Высокоомный резистор (R3) выполняет роль разряда конденсаторов C1 и C2 при выключении питания для повышения безопасной эксплуатации и обслуживания устройства ремонтным персоналом. Защитный варистор VR1 служит защитой от высоковольтных импульсных помех. На основе элементов L1, L2, C1, C2 выполнена частотно-зависимая цепь, реализующая подавление помех.

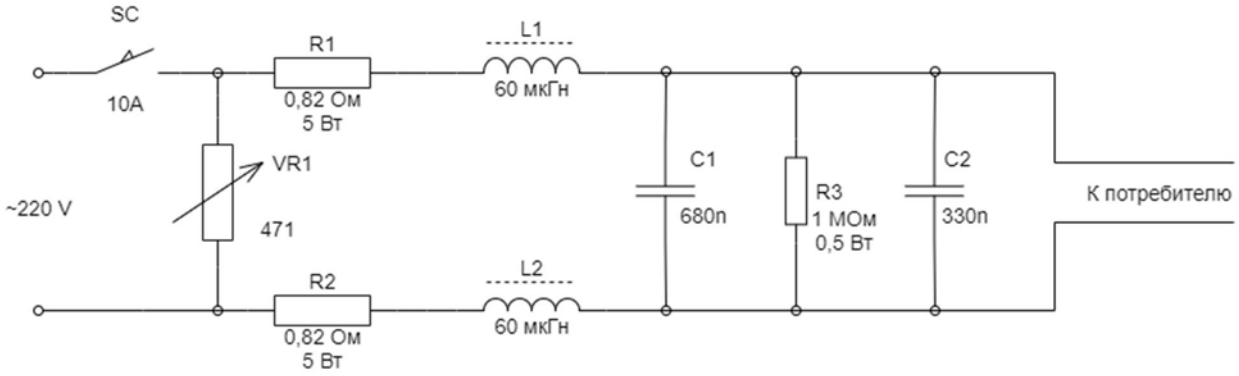


Рис. 2. Схема фильтра входного блока

Разработанная на функционально-логическом уровне математическая модель базируется на основе преобразования Лапласа и может быть записана в виде:

$$H(f) = \frac{R_{C\text{общ}(f)}}{\left(R_1 + R_{L1(f)} + R_{C\text{общ}(f)} + R_{L2(f)} + R_2\right)}, \quad (1)$$

где

$$R_{L1} = 2\pi f L_1, R_{L2} = 2\pi f L_2,$$

$$R_{C\text{общ}} = \frac{1}{2\pi f C_{\text{общ}}},$$

$$C_{\text{общ}} = C_1 + C_2.$$

Исследование модели фильтра удобнее всего осуществлять в каком-либо современном математическом пакете, например, Mathcad или Mathlab. В инженерных исследования наиболее привлекательным из этих двух программ является Mathcad, поскольку допускает возможность записи программ в виде формул в символьном виде.

Результат моделирования представлен на рис. 3.

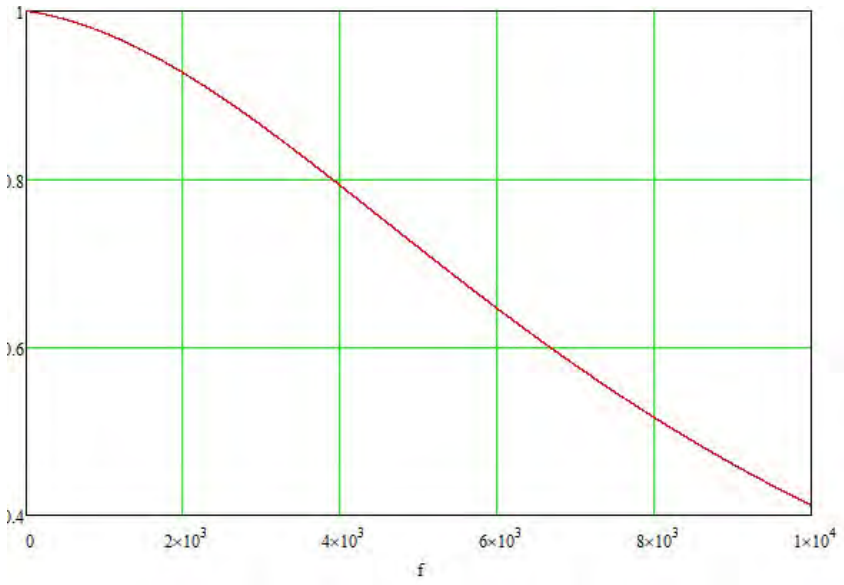


Рис. 3. График передаточной функции, где $f_{пм}$ = 1 Гц...10 кГц

Как следует из рис. 3, на частоте в 10 кГц ослабление сигнала помехи происходит более чем наполовину. Это позволяет говорить о том, что фильтр эффективно выполняет поставленную задачу.

Подводя итог следует отметить, что в рассматриваемой статье была представлена разработанная структурная схема новой адаптивной системы электропитания для АСУ, реализующая такие преимущества по сравнению с обычными СЭП как: модульность конструкции и приспосабливаемость к изменениям внешней среды.

Был произведен выбор математического аппарата для разработки математической модели фильтра помех входного блока системы, а также осуществлен ее анализ в среде математического моделирования Mathcad, подтвердивший возможность корректной оценки подобных устройств новой СЭП.

Также следует отметить, что представленная в настоящей статье информация может представлять интерес для широкого круга специалистов.

Список используемых источников

1. Белоусов О. А., Муромцев Д. Ю. Электропитание систем радиосвязи: учебное пособие. Тамбов: Изд-во ФГБОУ ВО «ТГТУ», 2016. 84 с. ISBN 978-5-8265-1533-4.

2. Anadigm, the dpASP company. URL: https://anadigm.com/ (дата обращения 15.01.2021).

3. Сетевые фильтры – как они работают. URL: https://radiostorage.net/4817-setevye-filtry-kak-oni-rabotayut-primery-skhem.html (дата обращения 19.02.2021).

Статья представлена заведующей кафедрой ИСАУ СПбГУТ, доктором технических наук, профессором Г. В. Верховой.

УДК 004.094.5
ГРНТИ 20.51.23

ОЦЕНКА ЭФФЕКТИВНОСТИ ПОДСИСТЕМЫ ВИЗУАЛИЗАЦИИ СРЕДСТВ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

М. И. Варламов, А. Н. Цибуля

Академия Федеральной службы охраны Российской Федерации

В статье описана методика оценки эффективности подсистемы визуализации средств обнаружения вторжений на основе программного комплекса ELK Stack. Представлены алгоритм функционирования подсистемы, пример панели визуализации, основанной в результате проведенного анализа среди наиболее популярных средств обнаружения вторжений. Рассмотренная в данной работе методика оценки эффективности подсистемы визуализации, направленна на повышение производительности оператора по выявлению инцидентов безопасности.

средства обнаружения вторжений, подсистема визуализации, оценка эффективности.

В настоящее время существует необходимость в постоянной поддержке следующих свойств информации: ценность, доступность, целостность и конфиденциальность. Защиту информации необходимо обеспечивать на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации. Для решения данной задачи создаются средства защиты информации. Одним из них является средство обнаружения вторжений (СОВ) – совокупность программных, программно-аппаратных и аппаратных компонент, целевая функция которого заключается в автоматическом выявлении воздействий на контролируемую данным средством информационную инфраструктуру, которые могут быть классифицированы, как компьютерные атаки (КА).

Среди базовых функций СОВ [1] можно выделить функции, связанные со сбором данных со всех сенсоров в единую базу данных, выявлению наиболее важных событий безопасности по типу угроз и их опасности, формированию данных для визуального представления и вывод их на экранные формы через интерфейс оператора. Последние функции реализуются встроенной подсистемой визуализации СОВ, которая позволяет оператору защищаемого сегмента сети реагировать на выявленные события безопасности.

Проведенный анализ подсистем визуализации наиболее популярных сертифицированных ФСТЭК России СОВ позволил выявить следующие их особенности:

1. Использование различного количества элементов визуального представления (таблиц, графиков, диаграмм), количество которых варьируется от 2–3 до десятков;

2. Активное применение цвета для выделения наиболее важных событий;

3. Ограниченные, как правило, возможности по изменению состава и особенностей представления на экране оператора элементов визуализации.

Взаимодействие компонентов подсистемы визуализации

Способы визуального отображения информации в СОВ напрямую зависят от ее объёма, скорости изменения (в связи с тем, что СОВ, как правило, являются системами реального времени) и набора решаемых оператором задач. Для определения наиболее подходящих способов отображения можно использовать платформу Е3 [2]. Элементы платформы Е3, такие как выразительность, эффективность и результативность, дают возможность точно выстроить по порядку представления и задачи восприятия. Схема платформы Е3 представлена на рис. 1.

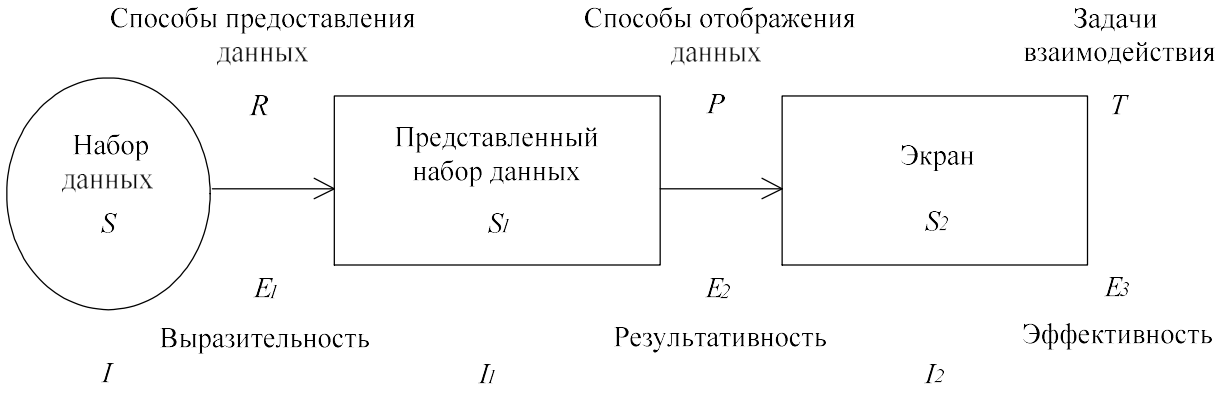


Рис. 1. Платформа Е3

Платформа Е3 для достаточно широкого круга задач может быть реализована на базе решений, заложенных в программный комплекс с открытым исходным кодом ELK Stack компании Elastic. Данный продукт состоит из следующих компонентов:

– Elasticsearch – нереляционная база данных (БД), состоящая из таблиц, именуемые «индексами», которые позволяют хранить события безопасности;

– Logstash – ПО, предназначенное для разбора (парсинга) входящих данных, поступаемых от сенсоров СОВ, для их преобразования и дальнейшей отправки в БД Elasticsearch;

– Kibana – панель визуализации событий безопасности, хранящиеся в Elasticsearch.

Структурная схема взаимодействия компонентов ELK Stack при реализации на их основе СОВ представлена на рис. 2.

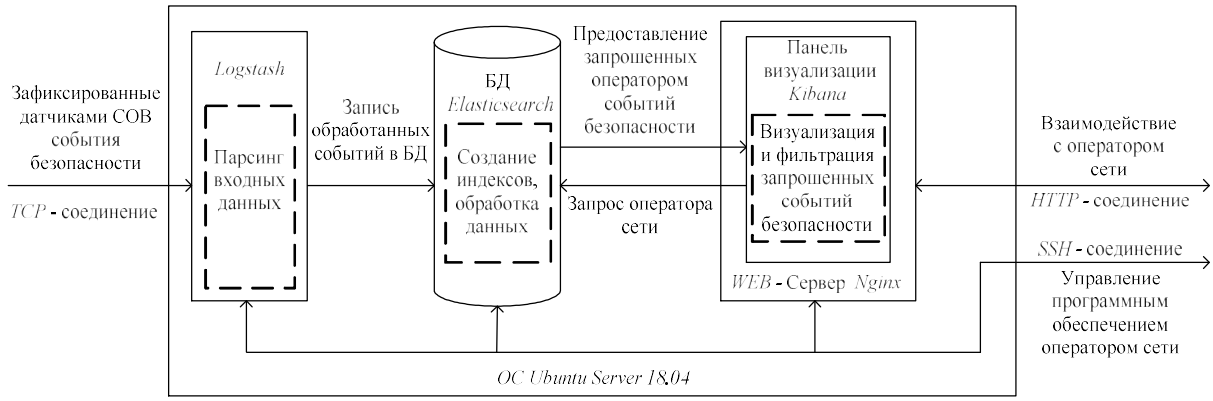


Рис. 2. Структурная схема взаимодействия элементов программного комплекса ELK Stack

Панель визуализации событий безопасности СОВ, созданная с использованием Kibana обладает достаточно широкими возможностями по созданию необходимого набора элементов визуализации на экране оператора. Пример панели визуализации представлен на рис. 3. Она включает:

– гистограмму активности, которая показывает количество зафиксированных датчиками СОВ сигнатур событий безопасности, отсортированных по возрастанию;

– гистограмму из 10 сигнатур, имеющих максимальное количество событий (топ-10), в столбцах которой изображены IP-адреса источников атак;

– графики количества зафиксированных событий по времени;

– круговую диаграмму скользящего окна, относительно количества поступивших событий (при настройке графика задаются пороги по скорости поступления событий безопасности);

– гистограмму 10 наиболее атакуемых портов.

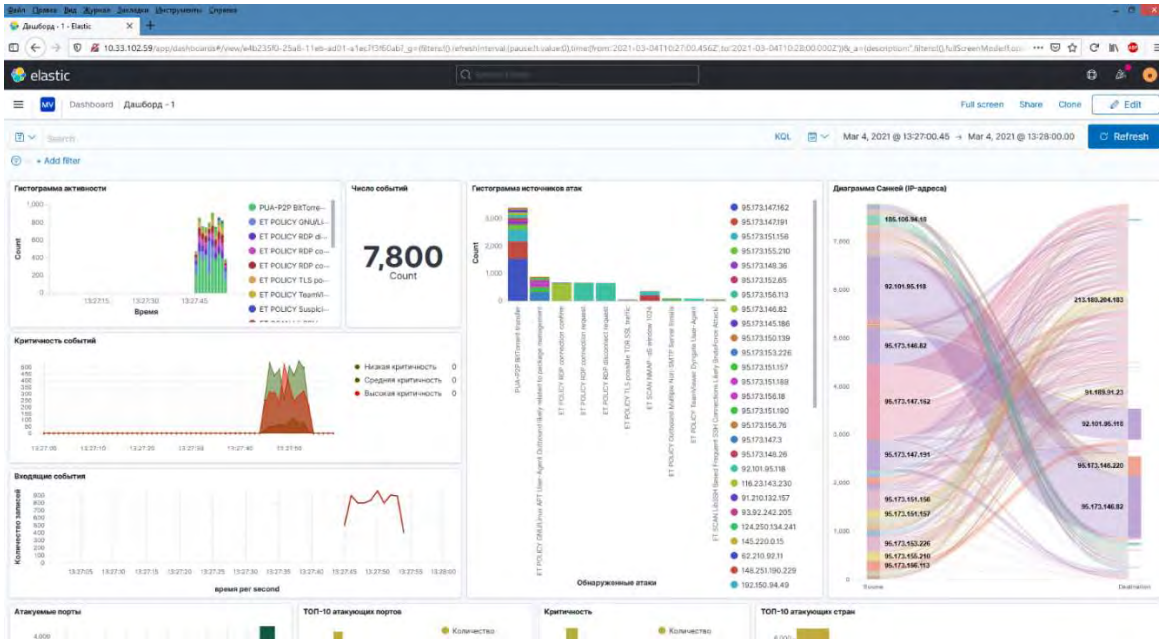


Рис. 3. Общий вид панели визуализации СОВ на базе ELK Stack

Оценка эффективности

Возникает задача оценки и сравнения эффективности использования различных средств отображения и их подмножеств. По аналогии с оценкой эффективности геоинформационных систем [3], можно для оценки качества визуализации использовать выражение:

$$k_Э = \frac{S_{\Sigma_{ЭВ}}\left(I, l_i, q_i, n_i\right) + S_{\Sigma_{РИ}}\left(J, u_j, o_j\right)}{S\left(L, H\right)}, \quad (1)$$

где I – число элементов визуализации;

l_i – длина i-го элемента визуализации;

q_i – ширина i-го элемента визуализации;

n_i – n-мерность i-го элемента визуализации;

L и H – линейные размеры экрана;

$S_{\Sigma ЭВ}$ – площадь на экране элементов визуализации, выводимых с учетом их размеров и n-мерности;

$S_{\Sigma РИ}$ – площадь на экране разнородной сопроводительной информации с учетом ее размеров;

J – число блоков разнородной описательной информации;

u_j – длина j-го блока разнородной сопроводительной информации;

o_j – высота j-го блока разнородной сопроводительной информации.

Данное выражение по сути представляет из себя оценку плотности элементов визуализации (с учетом их многомерности) и вспомогательной информации на экране оператора СОВ. В то же время эффективность подсистемы визуализации зависит не только от плотности покрытия экрана элементами, но и от их способности помочь оператору в необходимое время решить задачу обнаружения и верной интерпретации события безопасности. В связи с этим эффективность визуализации основывается также на качестве процесса анализа и восприятия оперативной информации. К частным показателям эффективности данного процесса можно отнести:

– наглядность (степень определяющая перегруженность или достаточность визуального представления информации);

– скорость искажений (скорость распознания информации как отдельных элементов, так и визуального представления в целом);

– время отклика (время необходимое человеку для принятия решения, на основе осмысленной информации).

Для оценки и определения наиболее эффективных способов реализации подсистемы визуализации СОВ будем учитывать алгоритм *SvEm* [4], который основан на теоретической оценке искажения, учитывающего сокращение

когнитивной нагрузки за счет смещения нагрузки на память оператора. В этой связи введем коэффициент $k_К$, рассчитываемый согласно выражению:

$$k_K = \frac{t_{\Sigma_{КП}}\left(I_{КП}, t_{КП_i}, n_{cl}\right)}{t_m}, \quad (2)$$

где $t_{\Sigma КП}$ – время, затраченное на определение всех необходимых параметров события безопасности с учетом использования элементов визуализации;

$I_{КП}$ – число элементов визуализации, использованных при когнитивном поиске;

$t_{КП}$ – время, потраченное оператором при взаимодействии с i-м элементом визуализации;

n_{cl} – число «кликов» необходимых для доступа к необходимой информации;

t_m – время, потраченное оператором при решении задачи распознавания без средств визуализации, с использованием его личного опыта.

Тогда общее выражение для оценки эффективности подсистемы визуализации центра обнаружения, предупреждения и ликвидации последствий компьютерных атак будет иметь вид: $K_{эф} = k_э / k_К$. Данное выражение имеет следующий физический смысл: чем более разнородной информацией, необходимой для распознавания события безопасности, заполнен экран, и чем меньше времени затратит оператор при использовании элементов визуализации, тем больший эффект от использования средства визуализации СОВ

Выводы

В работе представлена реализация программного комплекса подсистемы визуализации событий безопасности средства обнаружения вторжений. Также была описана методика оценки эффективности предоставляемой оператору информации. Благодаря данному подходу оператор способен быстрее обработать и проанализировать входящую информацию, а также корректно принять решение по недопущению или устранению инцидентов безопасности.

Список используемых источников

1. Информационное письмо Об утверждении требований к системам обнаружения вторжений: утв. ФСТЭК России 06.12.2011: ввод в действие 15.03.2012. URL: https://fstec.ru/normotvorcheskaya/poisk-po-dokumentam/118-tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/prikazy/394-informatsionnoe-pismo-fstek-rossii (дата обращения 16.11.2020).

2. Леунг Й. К., Апперли М. Д. E3: На пути к метрике методов графического представления больших наборов данных // Человеко-машинное взаимодействие: материалы междунар. науч. конф., Москва, 3-7 авг. 1993 г. М. : Springer, 1993. С. 125–140. URL: https://link.springer.com/chapter/10.1007/3-540-57433-6_44 (дата обращения 13.10.2020).

3. Зацаринный А. А., Воронин А. В., Ионенков Ю. С. Особенности оценки эффективности геоинформационной системы как элемента ситуационного центра // Системы и средства информатики. 2018. Том 26. N 3. С. 121-135. URL: https://elibrary.ru/item.asp?id=27177721 (дата обращения 11.10.2020)

4. Джефери Г., Райян К. Л. Ко, Марк А. Полномасштабный подход к измерению эффективности визуализации безопасности и презентации // Международная конференция IEEE по вопросам доверия, безопасности и конфиденциальности в вычислениях и коммуникациях : материалы 12-й международной конференции IEEE по науке и разработке больших данных (TrustCom / BigDataSE / ICESS), 2017. URL: https://ieeexplore.ieee.org/document/8029565/metrics#metrics (дата обращения 16.11.2020).

УДК 371.3
ГРНТИ 14.15.07

ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ ПОЛЬЗОВАТЕЛЬСКИХ ИНТЕРФЕЙСОВ СИСТЕМ ДИСТАНЦИОННОГО ОБУЧЕНИЯ ДЛЯ РАЗНЫХ КАТЕГОРИЙ ПОЛЬЗОВАТЕЛЕЙ

В. Д. Васильченко, Д. В. Волошинов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Дистанционное обучение является наиболее приоритетным для определенных категорий пользователей, в особенности для людей с инвалидностью и лиц с ограниченными возможностями здоровья. Наряду с этим, функциональные особенности пользовательских интерфейсов систем дистанционного обучения в таком случае должны обладать расширенным функционалом для удовлетворения потребностей пользователей. В статье рассматриваются основной и достаточный функционал для комфортного обучения посредством СДО разных категорий пользователей, имеющих инвалидность. Использование дополнительного функционала и современных технологических возможностей для реализации дистанционного обучения позволит сделать образование более доступным для широкой аудитории, а процесс обучения – более комфортным.

системы дистанционного обучения, электронные образовательные ресурсы, панель комфортного чтения, инвалидность, ограниченные возможности здоровья.

Современные технологии открывают все больше возможностей для более комфортного взаимодействия человека в самых разнообразных сферах деятельности. В том числе благодаря компьютеризации, процесс обучения стал не только более информативным и разнообразным, но и более доступным. Сейчас

высшее образование возможно получать, совмещая его с работой, другой учебой или даже находясь на другом конце земного шара. При этом студент может поступить сразу после школы или же быть пожилого возраста, учиться никогда не поздно. Все это стало доступно в том числе благодаря широкому распространению дистанционного обучения, которое принято считать выгодно отличающимся от более привычного заочного обучения.

Есть отдельная категория людей, которая долгое время оставалась практически незамеченной, и, в связи с этим, на нее было не принято ориентироваться по многим параметрам, в том числе при организации обучения. К этой категории относятся люди с инвалидностью и ограниченными возможностями здоровья, которые составляют более 12 % от общего количества населения России [1]. Таким образом, для данной категории студентов процесс обучения должен быть комфортен и доступен в полной мере, наравне с другими студентами. В зависимости от группы инвалидности, потребности у студентов могут отличаться, но если в образовательных учреждениях будет реализовано дистанционное обучение с поддержкой панели комфортного чтения, это позволит охватить если не большую, то значительную часть указанной категории студентов.

Адаптация дистанционной образовательной среды для выделенной категории студентов будет способствовать более широкому распространению СДО, более высокому качеству получаемого в заданных условиях образования, а также повышать доступность образования в целом. Для достижения поставленной цели необходимо планомерно развивать существующие системы дистанционного обучения, наполняя их необходимым функционалом: панелями комфортного чтения, возможностью непрерывно – в рамках учебного плана и расписания – взаимодействовать с преподавателем как в видео-, так и в текстовом формате – в зависимости от возможностей студентов, и другими функциями.

Для того, чтобы иметь представление об особенностях функционала систем дистанционного обучения и панели комфортного чтения, необходимо рассмотреть основные нарушения, свойственные людям с ограниченными возможностями здоровья и людям с инвалидностью. Среди основных форм нарушений можно выделить: нарушение слуха, зрения, речи, интеллекта, психического развития, опорно-двигательного аппарата и множественные нарушения. Панели комфортного чтения позволяют упростить процесс взаимодействия с СДО людям с нарушениями зрения, в то время как сами системы дистанционного обучения способствуют организации обучения для ряда других категорий студентов, в числе которых:

− люди с нарушением слуха и речи, позволяя осуществлять взаимодействие с преподавателями и изучать материал в текстовом формате;

− люди с нарушением интеллекта и психического развития, позволяя распланировать учебную программу с учетом особенностей студента, при этом сам

студент имеет постоянный доступ к материалам дисциплин и может изучать дополнительно при необходимости;

− люди с нарушением опорно-двигательного аппарата, позволяя проходить обучение из дома, без необходимости посещения образовательного учреждения и ручного конспектирования дисциплин.

Таким образом, для организации обучения средствами СДО для студентов, имеющих инвалидность, и студентов с ограниченными возможностями здоровья такие системы должны иметь определенные функциональные возможности. При этом стоит отметить, что наличие данного функционала также значительно упрощает процесс обучения и для других студентов [2]. Среди основного функционала можно выделить следующее:

− постоянный доступ к материалам дисциплин, в том числе для повторного изучения – наиболее значим для студентов с нарушением интеллекта;

− наличие сопроводительного материала – для лучшего освоения и большей наглядности;

− обмен сообщениями с преподавателями – особенно значимый пункт для студентов с нарушением слуха;

− обмен файлами с преподавателями для получения заданий и направления выполненных работ;

− интегрированные системы контроля знаний: тестирования и другие текстовые задания, в том числе в качестве эквивалента очным экзаменам и зачетам;

− видеосвязь с преподавателями – не подойдет для людей с нарушением слуха, но в целом является очень важной составляющей дистанционного обучения.

Помимо функционала систем дистанционного обучения, необходимо выделить ряд особенностей непосредственно организации процесса обучения: разделение информации на небольшие блоки для лучшего усвоения информации, распределение дисциплин в разрезе учебного года, а также участие в обучающем процессе преподавателей, чтобы студент имел возможность своевременно получать обратную связь [3].

Панели комфортного чтения широко распространены на сайтах общего пользования: информационных порталах, сайтах магазинов, государственных и негосударственных организаций и так далее, однако при этом в системах дистанционного обучения такие панели практически не используют. Формат панели комфортного чтения должен соответствовать требованиям аудитории, а все варианты настроек должны быть корректно отображены в СДО, сохраняя адаптивность системы. При этом сама кнопка доступа к панели комфортного чтения должна быть достаточно заметной и крупной. Таким образом, на панели комфортного чтения должны быть доступны следующие настройки:

− изображения: цветные, монохромные, без изображений;

− шрифт: размер, тип, межстрочный интервал, межбуквенный интервал;

− цвет: черный на белом, белый на черном, зеленый на темно-коричневом, темно-синий на голубом, коричневый на бежевом, наличие акцентов;

− дополнительный функционал: экранный диктор, текстовые пояснения, управление клавиатурой.

Подводя итоги, можно сделать вывод о том, что представленные функциональные возможности СДО в целом и панели комфортного чтения в частности позволят сделать процесс обучения наиболее комфортным для разных категорий студентов. Это позволит улучшить качество образования студентов с инвалидностью и ограниченными возможностями здоровья, при этом дисциплины будут доступны для освоения в полной мере без необходимости посещения образовательного учреждения. Системы дистанционного обучения на данный момент являются наиболее инновационным и перспективным форматом обучения, подходящим не только отдельным категориям студентов, но также людям, вынужденным совмещать получение образования с работой или обучением в другом образовательном учреждении, а также тем, кто по каким-либо причинам находится в другом городе или стране. Расширение и усовершенствование функционала систем дистанционного обучения и панели комфортного чтения может стать не только отправной точкой для улучшения качества образования студентов с инвалидностью и ограниченными возможностями здоровья, но и в целом положительно повлиять на распространение ДО как полноценной формы обучения.

Список используемых источников

1. Число инвалидов в России // interfax.ru: независимое информационное агентство. 1989. URL: https://www.interfax.ru/russia/686454 (дата обращения 17.03.2021).

2. Методические рекомендации для преподавателей по работе со студентами-инвалидами и студентами с ограниченными возможностями здоровья // ssuwt.ru: сайт СГУВТ. URL: http://www.ssuwt.ru/metod-rek-prep-inv (дата обращения 17.03.2021).

3. Рекомендации для преподавателей по работе со студентами с ограниченными возможностями здоровья и инвалидностью // hse.ru: сайт ВШЭ. URL: https://www.hse.ru/inclusive/recommendations (дата обращения 17.03.2021).

УДК 004.81
ГРНТИ 20.23.17

ИССЛЕДОВАНИЕ ПРОБЛЕМ СВОЕВРЕМЕННОГО ДОСТУПА К АКТУАЛЬНОЙ ИНФОРМАЦИИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

А. М. Велюго, Ф. В. Филиппов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Переход на цифровую экономику системообразующих корпораций и органов государственных служб, неэффективен без внедрения в периметр корпоративной информационной системы онтологических информационно-справочных web-сервисов. В статье описываются основные причины реализации собственного решения в рамках периметра корпоративной информационной системы, а также описан основной пайплайн преобразования данных в структурированный документ поисковой выдачи.

когнитивный поиск, корпоративная информационная система, обработка данных.

Обеспечение ускоренного внедрения цифровых технологий в экономике и социальной сфере является в России является одной из национальных целей развития (Указ Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», далее – Указ № 204). Для этого Указом № 204 определены следующие задачи:

1. Увеличение внутренних затрат на развитие цифровой экономики за счет всех источников (по доле в валовом внутреннем продукте) не менее чем в 3 раза по сравнению с 2017 г.;

2. Создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств;

3. Использование преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями [1].

Реализация данных целей возложено на национальный проект «Цифровая экономика» на период с 2019 по 2024 годы [2].

Большинство системообразующих предприятий, государственных органов и учреждений эксплуатируют корпоративные информационные системы. Корпоративные информационные системы (КИС) – это интегрированные системы управления территориально распределенной корпорацией, основанные

на углубленном анализе данных, широком использовании систем информационной поддержки принятия решений, электронных документообороте и делопроизводстве. КИС призваны объединить стратегию управления предприятием и передовые информационные технологии. Корпоративная информационная система – это совокупность технических и программных средств предприятия, реализующих идеи и методы автоматизации [3]. Использование корпоративных информационных систем обусловлено спецификой области деятельности различных предприятий и государственных органов, а также высоким требованиям к защите информации. Возможность внедрения on-premise решений позволяет решить типовые проблемы организации, например, учет заработной платы, службу технической поддержки (*service desk*). При этом они не решают узконаправленные проблемы, которые возникают не только в различных сферах деятельности, но и между различными дочерними обществами общей группы компаний. Для решения таких задач компании либо заключают договор на оказание услуг с иными организациями, либо формируют штат сотрудников для разработки и сопровождения корпоративной информационной системы.

Для решения узкоспециализированных задач на всех этапах жизненного цикла предприятия может быть создано множество информационных систем за большой период времени. Во время эксплуатации корпоративные информационные системы проходят непрерывную доработку функционала, особенно в тех случаях, когда применяется гибкая методология разработки.

Нередко случается такое, что одному сотруднику приходится работать сразу в нескольких информационных системах с одной и той же информацией.

По мере увеличения объемов организации, штата сотрудников, корпоративных информационных систем, увеличивается и объем информации, с которой работают пользователи.

Проблема поиска внутрикорпоративной информации является актуальной уже давно. Сотрудники тратят весомую часть рабочего времени на поиски документов [4]. В 70 % случаев сотрудники не знают существует ли актуальная информация в периметре корпоративных информационных систем, а в 30 % ищут сохраненный ранее документ [5].

Внешние поисковые системы, такие как Яндекс или Google, работают только с web-сайтами общедоступной сети Интернет и имеют большое количество пользователей, которые в достаточно короткие сроки позволяют обучить поисковые алгоритмы. Корпоративные информационные системы состоят из нескольких различных ресурсов, которые никак не связаны друг с другом: одни системы представлены в виде Интранет-ресурсов, другие – в виде исполняемого файла с двухфакторной аутентификацией, третьи – в виде каталога на сетевом ресурсе. Различные способы интеграций приводят к тому, что ограничиться реализацией лишь web-скрапингом не получится, необходимо также

разрабатывать собственное API (*application programming interface*), а также дополнительно предусмотреть возможность работы по протоколу SMB (*server message block*).

Получив образ документа из информационной системы, необходимо проанализировать его свойства. Нельзя заранее определить, что по API в систему придет метаданные html-страницы или rar-архива. Определив свойства документа, выбирается дальнейший алгоритм разбора содержимого.

Используя интеграцию через web-скрапинг или API с html-страницей, текстовые данные, скорее всего, часто приходят в заранее заданном формате. Возможно дополнительно придется произвести перекодирование данных в человеко-читаемый UTF-8. Если по интеграции приходит файл, например, в pdf формате, то необходимо прочитать его содержимое. Если у файла есть текстовый слой, то это облегчает весь алгоритм, но старые и подписанные документы чаще всего сканируются без него, поэтому дополнительно необходимо применять оптическое распознавание символов (OCR – *optical character recognition*). Кроме контента документа необходимо также собрать информацию по метаданным самого файла, такие как дата изменения и создания документа, автор документа, расположение файла и т. д. Все эти данные помогут целевому пользователю среди сотен тысяч документов компании отобрать именно тот, который нужен ему.

После того, как атрибутивный образ документа будет загружен в систему, следует произвести морфологический и синтаксический разбор. Необходимо построить числовой семантический вектор (*word embedding*) текстового образа файла, который позволит соотносить содержимое с поисковым запросом пользователя [6]. Из документа также можно выделить ключевые слова – наиболее частые слова/фразы в тексте либо их синонимы.

Используя предобученную модель машинного обучения, документам присваиваются определенные категории, например, приказ генерального директора, основополагающий стандарт предприятия, инструкция информационной системы и т. д.

Отдельным вызовом для поисковых систем в корпоративной информационной системе является наличие ролевых моделей – необходимо предоставлять доступ к закрытой информации только тем сотрудникам, у которых есть определенные права. Возможность передачи ролевого доступа зависит от типа интеграции, но, обычно, у каждого документа есть атрибут, отвечающий за доступ (может быть представлен в виде токена или базовой авторизацией, который в шифрованном виде сравнивается с данными пользователя поисковой системы).

Наконец, после получения всех атрибутивных и текстовых данных документа, строится полнотекстовый индекс для дальнейшего поиска в системе.

Таким образом, поисковая система в периметре корпоративной информационной системы должна иметь функционал:

1. Обновляемой интеграции с различными источниками данных;
2. Индексации сотен тысяч документов одновременно;
3. Распознавания текста в том числе из pdf-файлов и изображений;
4. Понимания корпоративного языка для формирования онтологий;
5. Проведения семантического анализа документов;
6. Структурирования данных по единым правилам;
7. Разграничения прав пользователей;
8. Интуитивно-понятного интерфейса, по аналогии с внешними поисковыми информационными системами.

Список используемых источников

1. Абдрахманова Г. И., Вишневский К. О., Гохберг Л. М. и др. Что такое цифровая экономика? Тренды, компетенции, измерение // XX Апр. междунар. науч. конф. по проблемам развития экономики и общества, Москва, 9–12 апр. 2019 г. М. : Изд. дом Высшей школы экономики, 2019. 82 с. URL: https://www.hse.ru/data/2019/04/12/1178004671/2%20 Цифровая_экономика.pdf (дата обращения 30.03.2021).

2. Цифровая экономика России 2024. URL: https://data-economy.ru/#rec38557658 (дата обращения 30.03.2021).

3. Корпоративные информационные системы. URL: http://iablov.narod.ru/igupit/kislec.htm (дата обращения 30.03.2021).

4. Сколько времени сотрудники компаний тратят на поиск информации. URL: https://www.bckspc.com/skolko-vremeni-sotrudniki-kompanij-tratyat-na-poisk-informacii/ (дата обращения 30.03.2021).

5. Технологии против разгильдяйства: как умный поиск меняет бизнес. URL: https://www.forbes.ru/tehnologii/369757-tehnologii-protiv-razgildyaystva-kak-umnyy-poisk-menyaet- biznes (дата обращения 30.03.2021).

6. Что такое эмбеддинги и как они помогают машинам понимать тексты. URL: https://ai-news.ru/2020/03/chto_takoe_embeddingi_i_kak_oni_pomogaut_mashinam_ponimat_teksty.html (дата обращения 30.03.2021).

Статья представлена научным руководителем,
кандидатом технических наук, старшим научным сотрудником,
доцентом Ф. В. Филипповым.

УДК 004.421
ГРНТИ 28.19.23

ИССЛЕДОВАНИЕ И РАЗРАБОТКА ОСТРОВНЫХ МОДЕЛЕЙ НЕБЛОКИРУЮЩИХ МНОГОПОТОЧНЫХ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ ОПТИМИЗАЦИИ ДЛЯ СТАНКОВ С ЧИСЛОВЫМ ПРОГРАММНЫМ УПРАВЛЕНИЕМ

Г. В. Верхова, Д. С. Колесов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Оптимизация пути является распространённой задачей нынешнего времени, так как сложность такой задачи многократно возрастает с ростом точек маршрута. Для решения проблем оптимизации пути, обычно используются эвристические алгоритмы. В работе исследована и разработана островная модель неблокирующих многопоточных генетических алгоритмов оптимизации пути для станков с числовым программным управлением, проведены эксперименты и вычислено время ускорения работы алгоритма.

генетический алгоритм, исполнительный механизм, оптимизация траектории, операторы, кроссинговер, мутация, машинное обучение.

Благодаря своей структуре генетические алгоритмы имеют большой потенциал для разбиения на параллельные процессы, так как представляют собой совокупность отдельных решений, имеющих возможность обрабатываться независимо друг от друга [1]. Наибольшим препятствием для эффективного распараллеливания генетического алгоритма является реализация оператора отбора, так как он оперирует большой группой особей одновременно, а для некоторых функций отбора используются группы, состоящей из особей, которые в совокупности представляют всю популяцию, что создаёт узкое место в работе алгоритма.

Другие операторы таких особенностей не имеют [2]. Для процесса скрещивания необходимо разбить всех особей популяции на пары, которые могут быть обработаны параллельно друг от друга. Для реализации оператора мутации, взаимодействие между различными особями популяции не требуется, так как каждая из них, в отрыве от остальных, самостоятельно «принимает решение» о своей мутации с заданной вероятностью [3].

Параллельное выполнение генетического алгоритма можно добиться с помощью использования островной модели (рис. 1), суть которой заключается в том, что вся популяция генетического алгоритма разбивается на некоторое число меньших популяций, расположенных на отдельных островах, и каждая

изолированная популяция обрабатывается в отдельном вычислительном потоке по обычным правилам, независимо друг от друга [4]. Чтобы избежать простого выполнения нескольких копий генетического алгоритма параллельно, необходимо организовать обмен информацией между различными группами, для чего вводится оператор миграции. Данный оператор производит обмен особями между соседними группами через каждые *N* шагов выполнения генетического алгоритма. Изменяя количество особей и частоту выполнения обмена, можно управлять степенью миграции, создавая малую и большую коммуникационную нагрузку. Такой параллелизм позволяет использовать различные варианты генетического алгоритма на каждом вычислительном потоке, что позволит лучше избегать зацикливания алгоритма в локальных экстремумах.

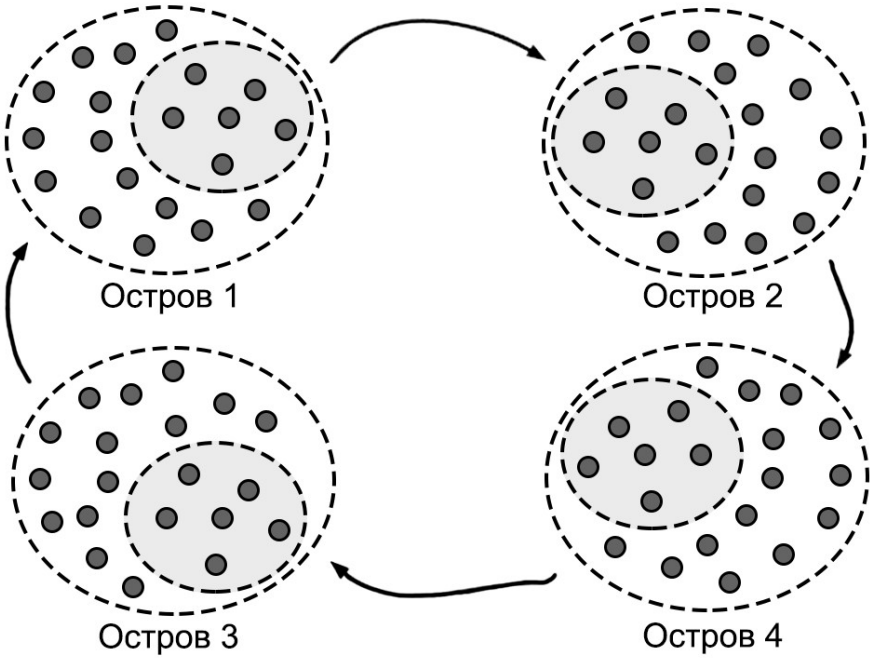


Рис. 1. Островная модель генетического алгоритма

Из-за несинхронной обработки данных на разных островах, происходят ситуации, когда популяция не может мигрировать с одного острова на другой, так как алгоритм второго острова будет находиться в рабочем состоянии, что вызовет блокировку работы первого алгоритма. Для решения этой проблемы, необходимо усовершенствовать модель и ввести промежуточные острова (рис. 2), которые будут выступать буфером для особей на обмен, чтобы один поток имел возможность перебросить особей в буфер и продолжить работу, не дожидаясь завершения фазы работы соседних потоков.

Был проведён ряд вычислительных экспериментов генетического алгоритма, распараллеливаемого с помощью модифицированной островной модели [5], в ходе которых выявлено, что расхождение между фазами соседних

островов наиболее вероятно будет в пределах 10–20 % от времени работы одного полного решения алгоритма (рис. 3).

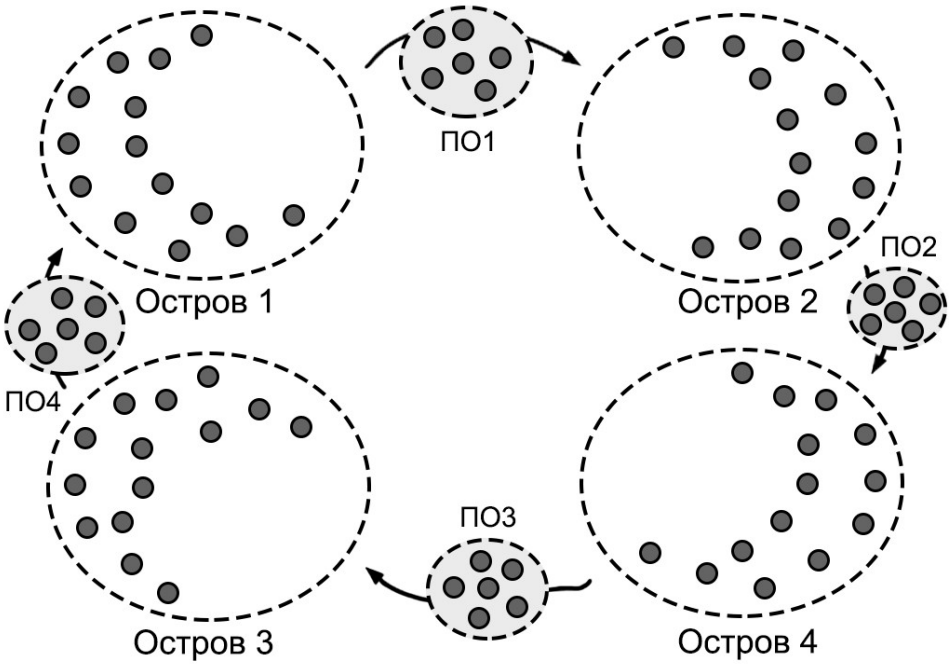


Рис. 2. Модифицированная островная модель генетического алгоритма

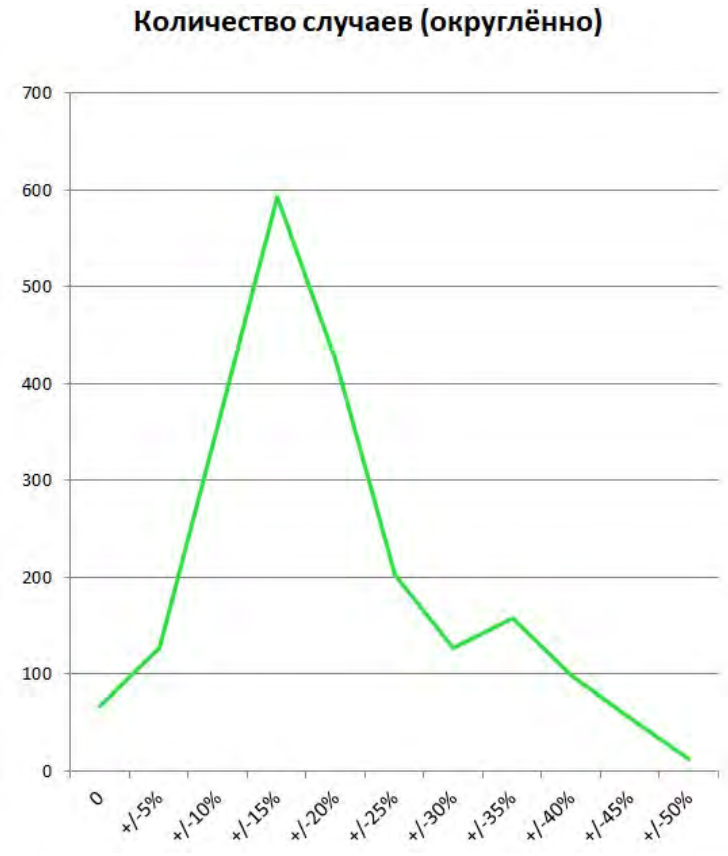


Рис. 3. Количественные результаты эксперимента

Для разного оборудования количество значимых циклов, на которых можно будет заметить разницу во времени работы, будет отличаться. Были проведены эксперименты по работе алгоритма с блокирующей и неблокирующей моделью со значимым количеством циклов на компьютере с процессором *Intel Core i7-8750H,* имеющим 6 ядер и 12 рабочих потоков. Результаты представлены в таблице.

ТАБЛИЦА. Сравнение двух моделей генетического алгоритма

Номер эксперимента	**1**	**2**	**3**	**4**	**5**
Блокирующая модель, с	3,22	4,5	3,91	3,7	3,45
Неблокирующая модель, с	2,9	2,78	3,11	2,53	2,42

На основе данных эксперимента, был высчитан выигрыш во времени, на основе математических ожиданий времени работы блокирующей (1) и неблокирующей (2) моделей.

$$M_1 = \frac{3{,}22+\ {,}5+3{,}91+\ {,}7+3{,}45}{5} = 3{,}756, \quad (1)$$

$$M_2 = \frac{2{,}9+2{,}78+\ {,}11+\ {,}53+\ {,}42}{5} = 2{,}748. \quad (2)$$

Выигрыш во времени работы составил $1 - \frac{M_2}{M_1} \approx 26\ \%$.

Список используемых источников

1. Ikotun, A. M.; Lawal, O. N.; Adelokun, A. P. The Effectiveness of Genetic Algorithm in Solving Simultaneous Equations // International Journal of Computer Applications, vol. 14. No. 8. February 2011.

2. Alba, E.; Dorronsoro, B. Cellular Genetic Algorithms. Operations Research // Computer Science. Vol. 42. Springer, Heidelberg. 2008.

3. Колесов Д. С. Операторы мутации и кроссинговера для решения задачи оптимизации траектории движения исполнительного механизма с помощью генетических алгоритмов // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2020). Региональная научно-методическая конференция магистрантов и их руководителей; Сб. луч. докл. конф. СПб.: СПбГУТ, 2021. С. 285–289.

4. Ершов Н. М. Естественные модели параллельных вычислений. Лекция 9. Генетические алгоритмы // Суперкомпьютерное образование. Интернет-центр системы образовательных ресурсов в области СКТ. 2011. 14 с. URL: http://hpc-education.ru/files/lectures/2011/ershov/ershov_2011_lectures09.pdf

5. Верхова Г. В., Акимов С. В., Фёдоров Н. С., Хвостов М. А., Купцов А. В. Программное обеспечение для оптимизации траектории движения исполнительного механизма станка с ЧПУ // Свидетельство о регистрации программы для ЭВМ 2020664178, 09.11.2020. Заявка № 2020663414 от 29.10.2020.

УДК 004.421
ГРНТИ 50.41.29

ПРОГРАММНО-АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ВИЗУАЛИЗАЦИИ ПРОЦЕССА РЕШЕНИЯ ОПТИМИЗАЦИОННЫХ ЗАДАЧ С ПОМОЩЬЮ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ

Г. В. Верхова, А. В. Купцов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Компьютерная графика представляет собой современный эффективный метод анализа научных данных. В данной работе предлагается реализация алгоритма визуализации функционирования генетического алгоритма в режиме реального времени. Генетический алгоритм служит для оптимизации траектории движения лазера станка с числовым программным обеспечением.

визуализация, оптимизация, генетические алгоритмы, программирование, эволюционные вычисления.

Отличительной особенностью станков с числовым программным управлением (ЧПУ), предназначенных для лазерной резки металлов, является высокая точность и эффективность работы [1, 2]. С другой стороны, такие системы при работе потребляют большое количество электроэнергии, что сказывается на себестоимости продукции, а также имеет высокую стоимость оборудования и обслуживания. Учитывая сказанное, экономически эффективное расходования ресурса оборудования станка с ЧПУ является одной из первоочередных задач. Повышение эффективности расходования ресурсов станка с ЧПУ, снижения уровня энергопотребления и временных затрат может быть достигнуто с помощью генетического алгоритма. Разработанный генетический алгоритм решает задачу оптимизации траектории движения исполнительного механизма станка с ЧПУ [3].

Повышение степени информативности при анализе результатов работы генетического алгоритма требует наличия удобного интерактивного графического интерфейса. Такой интерфейс должен обладать следующими возможностями:

– отображать текущие параметры генетического алгоритма с возможностью их изменения;

– создавать интуитивно понятную схему оптимизируемой траектории (включая информацию о последовательности обработки сегментов);

– загружать конфигурацию оптимизируемого объекта из файла;

– сохранять и загружать результаты работы алгоритма для их последующей обработки.

Программа, реализующая генетических алгоритм [4], функционирует итерационно, формируя на каждой итерации последовательный набор сегментов. В каждом сегменте содержится информация о его начале, конце, а также направлении его обхода при обработке. В последовательности сегментов, представленной хромосомой, содержится информация о порядке обхода, где первый сегмент является началом. Диаграмма классов, предназначенных для представления сегментов, показана на рис. 1.

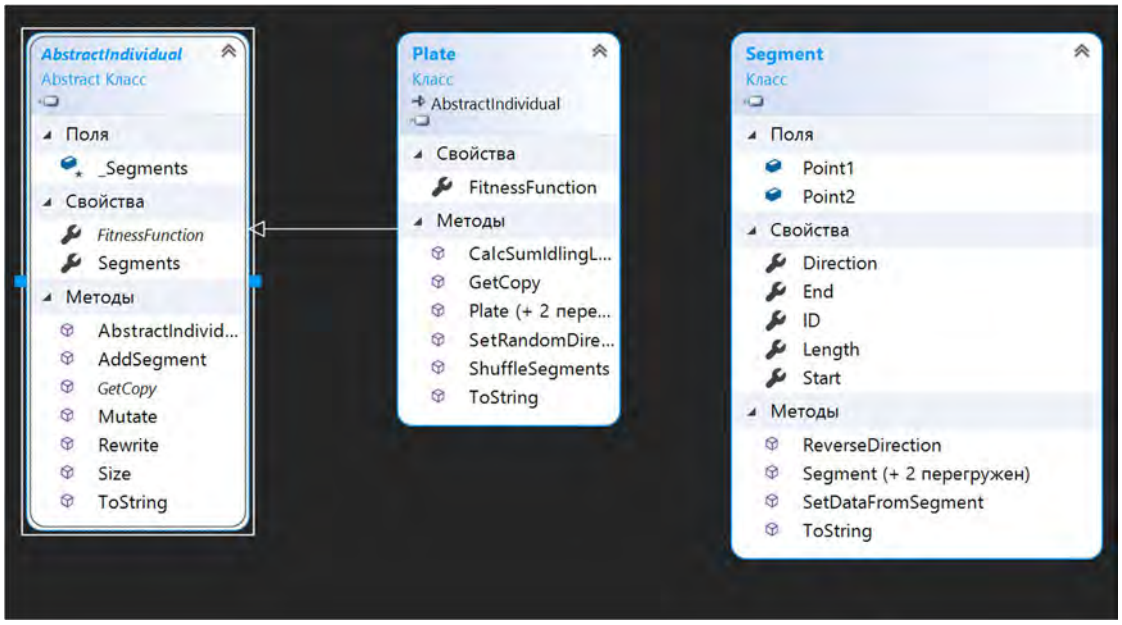


Рис. 1. Диаграмма классов, предназначенных для представления сегментов

Архитектура системы содержит два модуля, в которых реализованы независимые потоки исполнения (рис. 2.)

Рис. 2. Архитектура системы

Использование таймера задержки позволяет регулировать скорость выдачи результатов работы алгоритма пользователю. Графический интерфейс программы визуализации реализован с использованием языка объектно-ориентированного программирования C# и технологии WPF (*Windows Presentation Foundation*), которая является графической подсистемой с открытым исходным кодом [2]. Основной особенностью WPF является отделение пользовательского интерфейса от бизнес-логики.

Графический интерфейс состоит из трёх основных блоков (рис. 3):

– панель инструментов, где находятся основные элементы управления (кнопки паузы, импорта топологии и экспорта описания полученной траектории, а также элементы, позволяющие управлять генетическим алгоритмом);

– рабочая область, на которой схематически отображается эволюция траектории движения генетического алгоритма, с изменения масштаба отображения и области просмотра;

– консоль, в которой выводится лог работы генетического алгоритма.

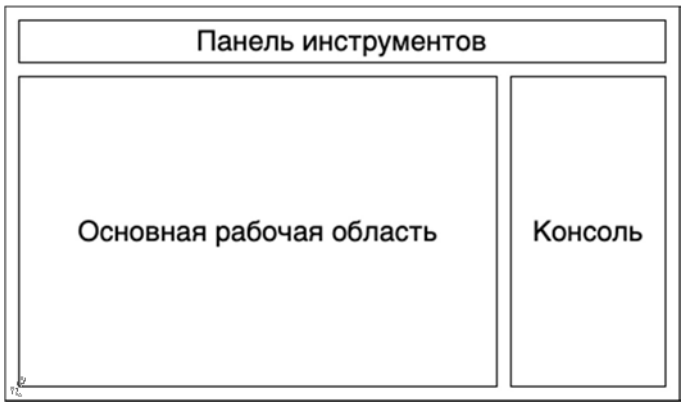
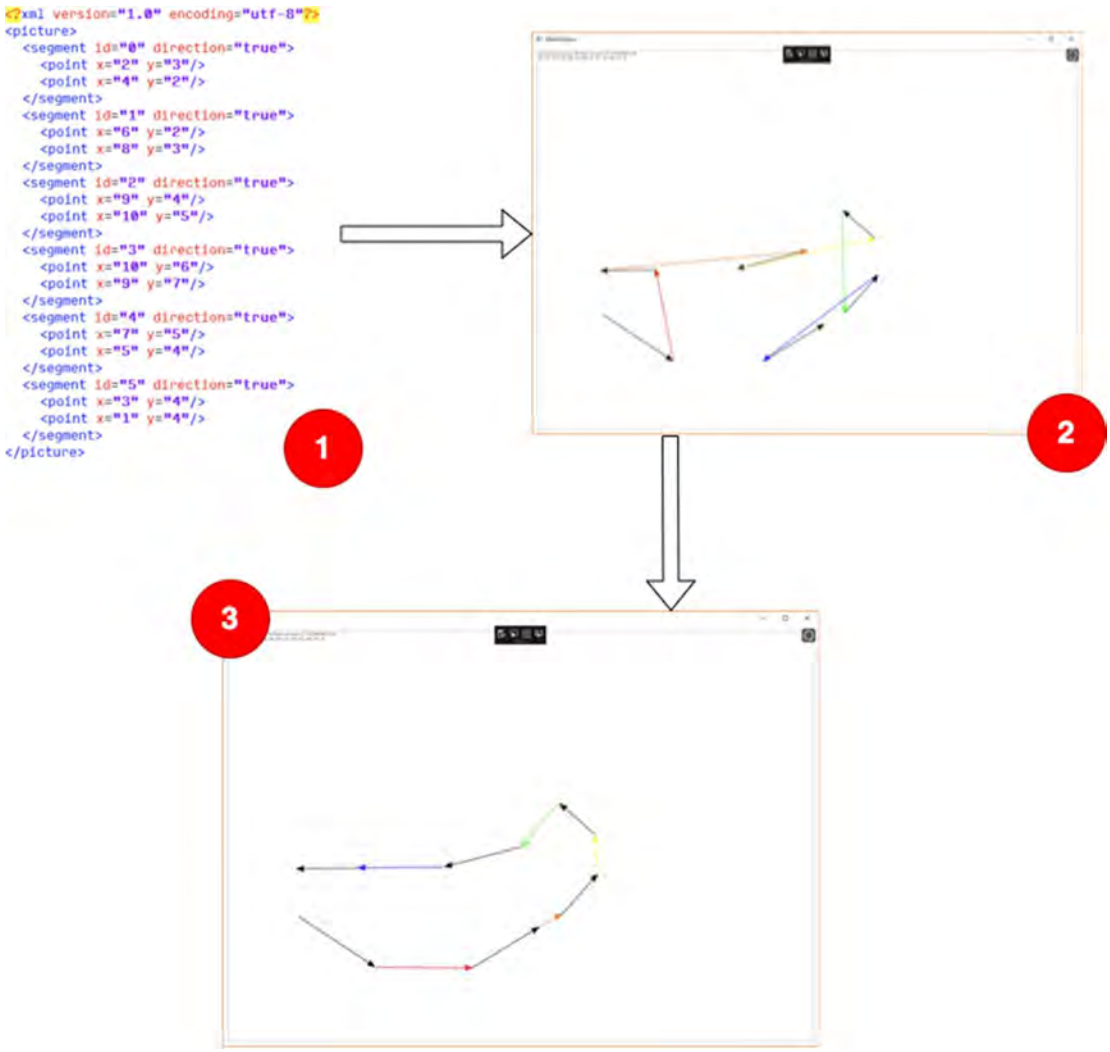


Рис. 3. Структура главного окна системы визуализации

Порядок работы с программным обеспечением производится следующим образом: загружается объект оптимизации из файла XML (рис. 4.1), инициализируются параметры генетического алгоритма (рис. 4.2) и он начинает свою работу. На рис. 4.2 и 4.3 представлен процесс работы генетического алгоритма. Цветными линиями отображается траектория движения исполнительного механизма в режиме холостого хода, при котором обработка не производится. Цветовая кодировка выполнена на основе спектра и определяет последовательность обхода, соответственно последовательности спектральных линий (от красной к фиолетовой), что дает наглядное представление функционирования генетического алгоритма, минимизирующего холостой ход. На рис. 4 продемонстрировано последовательное улучшение траектории движения исполнительного механизма (на рис. 4.2 длинна траектории движения исполнительного механизма значительно больше, чем на рис. 4.3).


<?xml version="1.0" encoding="utf-8"?>
<picture>

<point x="2" y="3"/>
<point x="4" y="2"/>

<point x="6" y="2"/>
<point x="8" y="3"/>

<point x="9" y="4"/>
<point x="10" y="5"/>

<point x="10" y="6"/>
<point x="9" y="7"/>

<point x="7" y="5"/>
<point x="5" y="4"/>

<point x="3" y="4"/>
<point x="1" y="4"/>

</picture>
1
2
3

Рис. 4. Графическое отображение работы программы

Список используемых источников

1. Технология лазерной резки металла. URL: https://www.metobr-expo.ru/ru/articles/tehnologiya-lazernoy-rezki-metalla/ (дата обращения 18.11.2020).

2. Лазерная резка металла. URL: https://svarkalegko.com/tehonology/lazernaya-rezka-metalla.html (дата обращения 18.11.2020).

3. Акимов С. В., Афанасьев М. Я., Меткин Н. П., Федосов Ю. В. Оптимизация траектории лазерной обработки плоскостных заготовок для МЭМС // Нано- и микросистемная техника. 2018. Т. 20. № 3. С. 145–157.

4. Верхова Г. В., Акимов С. В., Фёдоров Н. С., Хвостов М. А., Купцов А. В. Программное обеспечение для оптимизации траектории движения исполнительного механизма станка с ЧПУ // Свидетельство о регистрации программы для ЭВМ 2020664178, 09.11.2020. Заявка № 2020663414 от 29.10.2020.

5. Верхова Г. В., Акимов С. В., Фёдоров Н. С., Хвостов М. А., Купцов А. В. Программное обеспечение для визуализации работы генетического алгоритма // Свидетельство о регистрации программы для ЭВМ 2020664310, 11.11.2020. Заявка № 2020663375 от 29.10.2020.

УДК 004.896
ГРНТИ 28.23.27

МЕТОДЫ СИНХРОННОЙ ЛОКАЛИЗАЦИИ И ПОСТРОЕНИЯ КАРТ ДЛЯ АВТОНОМНЫХ ТРАНСПОРТНЫХ СРЕДСТВ

Г. В. Верхова, П. А. Прокофьев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Представлены результаты исследований методов одновременной локализации и построения карт для автономных транспортных средств. Выполнен сравнительный анализ методов SLAM. Рассмотрены пути построения библиотек программно-алгоритмического обеспечения методов локализации, построения и обновления геоинформационных многоаспектных моделей. Показано, что в настоящий момент времени для компактных беспилотных наземных транспортных средств в большинстве случаев предпочтительными представляются методы, использующие информацию, полученную с лидара. Рассмотрены пути интеграции гетерогенной информации в бортовом компьютере беспилотного транспортного средства с помощью многоаспектных моделей.

локализация, построение карт, автономные транспортные средства, SLAM, ROS.

Методы SLAM (*Simultaneous Localization and Mapping*) направлены на синхронную локализацию и построение карты для автономных беспилотных транспортных средств. Методы SLAM обеспечивают сбор информации с различных сенсоров и создание на базе данной информации карты местности с отображением на данной карте позиции транспортного средства.

В роли источников входных данных выступают лазерные дальномеры (лидары), монокулярные камеры и стереокамеры, камеры глубины, одометры, гироскопы и другие устройства. Выходная информация может быть представлена в виде карты или 2D-матрицы, в которой каждой ячейке присваивается вероятность того, что данная ячейка занята. Свободные ячейки отображаются белым цветом, занятые ячейки отображаются черным. Градации серого цвета отражают вероятность того, что текущая ячейка окажется занятой (чем выше вероятность того, что ячейка занята, тем более темным цветом она отображается на изображении [1]).

Существуют алгоритмы SLAM, которые строят графы перемещений автономного транспортного средства [2]. В данных графах ребра представляют собой векторы перемещений, а вершины содержат информацию, полученную с сенсоров автономного транспортного средства из точек, которые эти вершины

представляют. Возможно построение облаков точек, которые отражают положения объекта в пространстве с возможностью отображения вероятности того, что ячейка занята.

Существует большое количество методов SLAM, классифицируемых по разным критериям [3]. В таблице приведены наиболее распространенные методы SLAM, распределенные по типам входных данных.

ТАБЛИЦА. Сравнение характеристик методов SLAM

Метод	Камера			LIDAR		Одометрия
	Моно	Стерео	RGBD	2D	3D	
TinySLAM				x		x
GMapping				x		x
HectorSLAM				x		
Cartographer				x	x	x
ORB-SLAM	x	x	x			
RTAB-Map		x	x	x	x	x
S-PTAM		x				
PTAM	x					
SVO	x					
DPPTAM	x					
LSD-SLAM	x					
DSO	x					

В работе [4] приведены результаты сравнительного анализа некоторых из представленных в таблице методов для закрытого офисного помещения с одноцветными стенами. Алгоритм TinySLAM допускает самую компактную реализацию среди рассмотренных методов, поэтому подходит для систем с ограниченными вы вычислительными ресурсами, но обладающий низкой достоверностью в построении карты, что установлено в исследованиях [2].

В ряде работ приведены результаты исследований методов, основанных на получении информации от различных лазерных дальномеров, монокулярных камер, стереокамер и адометров [5, 6, 7]. В этих исследованиях было установлено, что GMapping не обеспечивает надежные результаты при построении карты. Траектории движения, построенные с помощью Hector SLAM и Cartographer, практически совпадают, что позволяет сделать вывод, что методы работают со сравнительно одинаковой точностью в заданных условиях, но их нельзя использовать в любых условиях, так как на данный момент не существует универсального метода SLAM. Каждая задача синхронной локализации и построения карт для автономных транспортных средств? требует выбора конкретного алгоритма, подходящего для решения данной задачи.

Методы, использующие монокулярные камеры обеспечивают представление информации для локализации объекта и построения карты, однако для восстановления абсолютного масштаба требуется использовать дополнительные типы датчиков. Методы, использующие стереокамеры предоставляют метрическую информацию о локализации транспортного средства, и могут полноценно использоваться для решения задач SLAM, при этом максимальную точность обеспечивают методы RTAB map, ORB SLAM и S-PTAM.

Реализация алгоритмов методов SLAM может быть реализована на базе платформы ROS – Robot Operating System (операционная система для роботом). Платформа ROS включает в себя набор библиотек, драйверов и интерфейсов моделирования, обеспечивающие возможность реализации проектов робототехнических средств. Платформа ROS функционирует под управлением операционной системы Linux, является свободно распространяемой и имеет открытые исходные коды [8].

Список используемых источников

1. Филатов Ар. Ю., Филатов Ан. Ю., Кринкин К. В., Чен Б., Молодан Д. Методы сравнения качества 2D-SLAM-алгоритмов // Известия СПбГЭТУ «ЛЭТИ». 2018. № 7. С. 87–95.

2. Филатов Ар. Ю., Филатов Ан. Ю., Гулецкий А. Т., Карташов Д. А., Кринкин К. В. Сравнение современных лазерных алгоритмов SLAM // Известия СПбГЭТУ «ЛЭТИ». 2018. № 7. С. 66–73.

3. Кузьмин М. Е. Классификация и сравнение существующих методов SLAM для групп роботов // VI Научно-практическая конференция с международным участием «наука настоящего и будущего» для студентов, аспирантов и молодых ученых. Сборник материалов конференции. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2018. С. 299–303.

4. Filipenko, M.; Afanasyev, I. Comparison of Various SLAM Systems for Mobile Robot in an Indoor Environment // 9th IEEE International Conference on Intelligent Systems 2018.

5. Grisetti, G.; Stachniss, C.; Burgard, W. Improved techniques for grid mapping with Rao-Blackwellized particle filters // IEEE Transactions on Robotics, vol. 23, no. 1, 2007. Pp. 34–46.

6. Pire T. et al. S-PTAM: Stereo Parallel Tracking and Mapping // Robotics and Autonomous Systems, vol. 93, 2017. Pp. 27–42.

7. Kohlbrecher, S., et al. A flexible and scalable SLAM system with full 3D motion estimation // 9th IEEE International Symposium on Safety, Security, and Rescue Robotics, SSRR 2011. Pp. 155–160.

8. Documentation ROS Wiki. UML: https://wiki.ros.org/ (дата обращения 23.02.2021).

УДК 681.518.5
ГРНТИ 28.15.23

МНОГОСЛОЙНАЯ СТРУКТУРА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА УПРАВЛЕНИЯ ПОДВОДНЫМ НЕОБИТАЕМЫМ АППАРАТОМ

Г. В. Верхова, Н. С. Фёдоров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Представлена многослойная структура программно-аппаратного комплекса управления автономным подводным необитаемым аппаратом. Показано, что предложенная многослойная структура обеспечит унификацию программно-алгоритмического и аппаратного обеспечения автономных подводных аппаратов при реализации различных функций управления (удержание местоположения подводного аппарата в условиях постоянного внешнего воздействия течения, автоматическое управление движением вдоль донной поверхности, имеющей сложный рельеф, движение аппарата по заданной траектории и т.п.). Предложенный подход обеспечит возможность гибкой комбинации различных алгоритмов управления автономным подводным аппаратом, а также адаптацию математического и программно-алгоритмического обеспечения под различные типы роботизированных подводных средств.

подводные необитаемые телеуправляемые аппараты, стабилизация, архитектура систем управления.

В настоящий момент времени актуальными задачами являются постоянная охрана акваторий, эффективное обслуживание подводных трубопроводом и телекоммуникационных кабелей, проведение подводных геолого-разведывательных работ, исследование и картография донной поверхности. Данные задачи могут быть эффективно решены с использованием автономных необитаемых подводных аппаратов [1]. Применение автономных необитаемых подводных аппаратов особо востребовано в условиях ограниченного пространства, затрудняющего ручное маневрирование, а также в условиях, при которых ошибка в ручном управлении может повлечь серьёзные последствия, например при работе с подводными кабелями и трубопроводами.

Для обеспечения эффективного выполнения широкого спектра задач в подводной среде, в состав АНПА входит большое количество датчиков, измерительных приборов и исполнительных механизмов, обычно выполняемых в формате модулей, устанавливаемых на шасси аппарата. Самыми распространёнными для установки на подводных аппаратах устройствами являются раз-

личные гидроакустические системы (гидролокаторы бокового и кругового обзора, эхолоты), датчики давления, видеокамеры, измерители расстояния до донной поверхности, гироскопы. Ввиду широкой номенклатуры модулей, технологий и решений, применяемых при их разработке, приходится работать с различными протоколами и форматами данных, которые используются для передачи информации от датчиков, а также для управления исполнительными механизмами.

В пределах одного модуля, имеющего несколько составных частей, обмен данными и командами может осуществляться по нескольким независимым каналам, организованным с использованием различных интерфейсов (SPI, CAN, Ethernet), в зависимости от требований к энергопотреблению, помехозащищённости и скорости передачи данных. Разнообразие протоколов, используемых в аппаратном обеспечении, предъявляет повышенные требования к встраиваемому программному обеспечению АНПА в части внутреннего информационного обмена [2].

Ввиду современной тенденции повышения универсальности применения создаваемых АНПА и постоянного расширение их возможностей, аппарат может выпускаться с множеством комбинаций устанавливаемых модулей, что усложняет процесс разработки встраиваемого программного обеспечения из-за необходимости внесения изменений для поддержки каждой конфигурации в отдельности. Решить описанные проблемы возможно при помощи использования многослойной архитектуры (рис. 1) при разработке программно-аппаратного комплекса АНПА.

Предлагаемая структура состоит из аппаратных модулей, входящих в состав АНПА и программных модулей преобразователей интерфейсов, модулей обработки и исполнительных модулей. Аппаратные модули, такие как манипуляторы, гидролокаторы, камеры с осветительными и поворотными устройствами, подключаются к вычислительной системе АНПА посредством соответствующих аппаратных интерфейсов. Входящие в состав встраиваемого программного обеспечения (ПО) АНПА программные модули преобразования интерфейсов позволяют получать данные по различным протоколам и преобразовывать их в универсальный формат для использования другими компонентами ПО. Применение такого слоя позволит использовать различные виды аппаратного обеспечения и заменять их без необходимости внесения изменений в программный код других слоёв системы.

Модули обработки, являющиеся программными модулями, которые осуществляют различные операции, такие как различные вычисления, фильтрация помех, усреднение, выработка команд, с данными, принимаемыми с преобразователей интерфейсов. Такими модулями являются регуляторы положения аппарата, обработчики данных гидролокаторов, камер, датчиков расстояния и давления. Результирующая информация поступает с модулей обработки в систему управления АНПА.

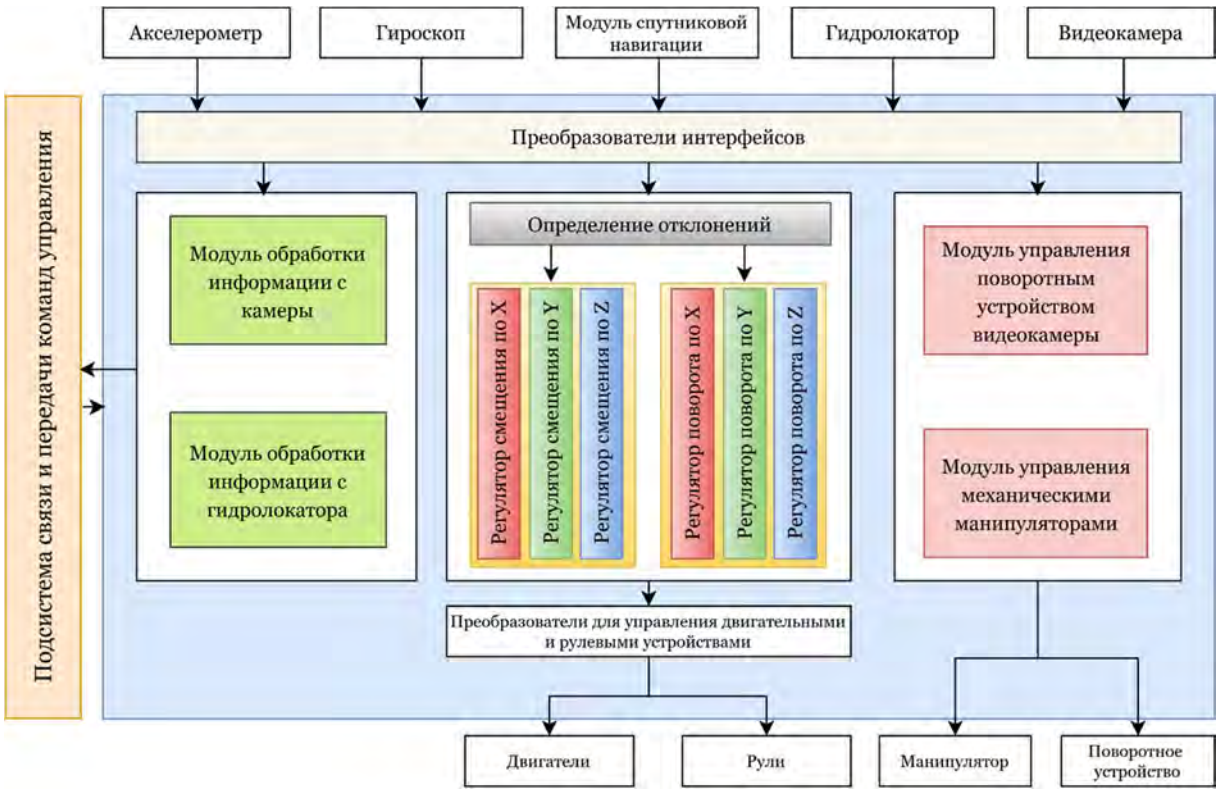


Рис. 1. Схема многослойной структуры программно-аппаратного комплекса АНПА

Система управления является главным компонентом, определяющим весь процесс функционирования АНПА, его возможности и реализуемые функции [3], поэтому разработка эффективной системы управления становится главной задачей в разработке всего комплекса встраиваемого программного обеспечения для АНПА. Требования, предъявляемые к системе управления, включают обеспечение выполнения поставленных задач на основе большого количества входных данных и ограничений, вызванных автономностью аппарата, характеристиками среды его функционирования, наличием внешних возмущающих воздействий, таких как подводные течения. Разрабатываемая система управления АНПА, должна обеспечивать универсальные для подводных аппаратов функции: движение по маршруту, выбор оптимальных режимов движения в зависимости от поставленной задачи и внешних условий, принятие решения о выполнении задачи, распознавание образов объектов, передача информации о выполняемых действиях и собственных параметрах.

Ограничение быстродействия, накладываемые допустимыми значениями размеров, массы и энергопотребления подводного аппарата, а также требования к скорости обработки получаемой информации и выработке управляющих воздействий часто требуют изменять распределение вычислительных ресурсов встраиваемой системы на различные операции в разных условиях. Также часто необходимо параллельное выполнение нескольких критических для корректного функционирования аппарата алгоритмов

Учитывая приведённые особенности, ограничения и требования, система управления выполняется как отдельный независимый слой программно-аппаратной структуры АНПА. Архитектура такого слоя приведена на рис. 2. Подсистема принятия решений будет обеспечивать заданную стратегию поведения, вырабатывая макрокоманды на основе данных, поступающих от модулей обработки. Макрокоманды представляют в декларативном виде требуемое от аппарата поведение в данной ситуации, например погружение, поворот или движение в определённую точку.

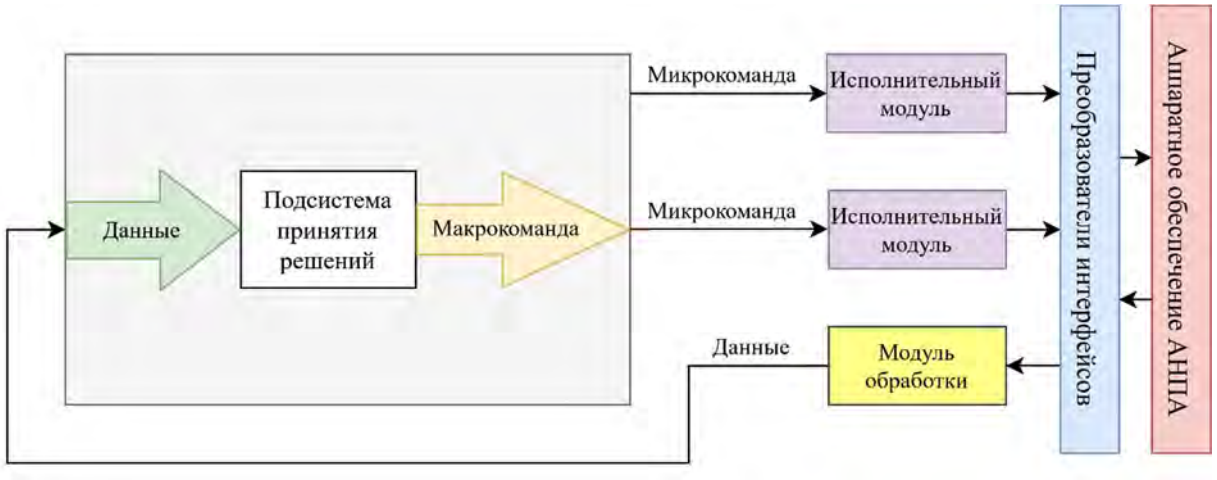


Рис. 2. Схема архитектуры системы управления АНПА

Системой управления макрокоманда будет разбита на микрокоманды, которые предписывают конкретные действия, которые необходимо совершить для выполнения макрокоманды, например включение двигателей, изменение плавучести, поворот рулей. Обработку микрокоманд осуществляют исполнительные модули, представляющие собой программно-алгоритмические модули, обеспечивающие преобразование микрокоманд в данные об управляющих воздействиях на исполнительные механизмы (двигатели, манипуляторы и т. п.). Исполнительные модули также обеспечивают контроль над исполнением микрокоманд соответствующими устройствами, позволяя получать отладочную информацию в случае их неисправности.

Многослойная структура позволит отделить алгоритмы преобразования входящей информации, алгоритмы регулирования и выработки управляющих воздействий, а также обеспечит возможность замены алгоритмов и настройки их параметров. Использование модулей преобразователей интерфейсов позволит применять различные виды аппаратного обеспечения без необходимости внесения изменений непосредственно в программный код. Путём изменения набора программных модулей уже существующее и отлаженное встраиваемое программное обеспечение можно будет использовать на АНПА, различающихся по аппаратной конфигурации.

Описанная архитектура системы позволяет добавлять дополнительные модули обработки и исполнительные модули для различных подсистем аппарата, таких как подсистема связи и передачи команд управления с внешнего пульта, система записи событий и данных, а также более эффективно распределять вычислительные ресурсы АНПА путём установки приоритетов выполнения алгоритмов различных модулей. Модули данной архитектуры можно разрабатывать и отлаживать независимо друг от друга и основной системы управления, что упрощает оптимизацию и тестирование программного обеспечения, а также позволяет предусмотреть замену модулей во время функционирования аппарата, многократно повышая универсальность и адаптивность аппарата к разным условиям внешней среды и поставленным задачам.

Список используемых источников

1. Пшихопов В. Х., Суконкин С. Я., Нагучев Д. Ш., Стракович В. В., Медведев М. Ю., Гуренко Б. В., Костюков В. А., Волощенко Ю. П. Автономный подводный аппарат «Скат» для решения задач поиска и обнаружения заиленных объектов // Известия ЮФУ. Технические науки. 2010. № 3 (104). С. 153–162.

2. Занин В. Ю., Кожемякин И. В., Потехин Ю. П., Путинцев И. А., Рыжов В. А., Семенов Н. Н., Чемоданов М. Н. Разработка автономных необитаемых подводных аппаратов класса микро с функцией группового управления // Известия ЮФУ. Технические науки. 2017. № 1-2 (186-187). С. 55–74.

3. Аллакулиев Ю. Б., Емелин В. И. Постановка проблемы управления автономными необитаемыми подводными аппаратами и формирование путей ее решения // Системы управления, связи и безопасности. 2018. № 4. С. 110–121.

УДК 004.946
ГРНТИ 50.49.31

МОДЕЛЬ КОМПЛЕКСИРОВАНИЯ АКАДЕМИЧЕСКОЙ КИБЕРСРЕДЫ

Г. В. Верхова, А. П. Шабанов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Представлены результаты исследований проблемы формирования единой цифровой экосистемы высшего образования и формирования на ее основе единого академического киберпространства. Показано, что формирование экосистемы требует наличия единой академической киберсреды, которая станет ее основой.

цифровая экосистема, единая академическая киберсреда, киберпространство, высшее образование.

В современном образовательном процессе высших и средних специальных учебных заведений существует тенденция по все более широкому внедрению электронной и дистанционной компонент, повышающие его доступность и эффективность [1, 2, 3, 4]. Проведение дистанционных лекционных и семинарских занятий представляет собой иной уровень взаимодействия между преподавателем и обучающимися. Электронные образовательные технологии способствуют повышению качества образовательного процесса, учету индивидуальных особенностей и предпочтений, а также формированию навыков самостоятельной работы.

В 2020 году в связи с пандемией новой коронавирусной инфекции бóльшая часть преподавателей и студентов временно была переведена на удаленный режим работы, но в виду того, что электронный документооборот и системы управления в современных вузах не позволяют выполнять все функции удаленно [5, 6], некоторые сотрудники были вынуждены выполнять свои обязанности в режиме оффлайн, что снижало степень самоизоляции.

Серьезной проблемой современного дистанционного образования в России является недостаток качественного контента, который позволил бы учащимся самостоятельно получать знания, а также отсутствие единого академического киберпространства, необходимого для обеспечения образовательного процесса на уровне, соответствующем современным требованиям. Формирование единого академического киберпространства обеспечит сквозную информационную поддержку основных образовательных программ на всех этапах жизненного цикла, сократит рутинные процедуры, включая предоставление возможности студентам готовить отчетные материалы и работать в формате виртуальных бригад.

Единая академическая киберсреда формируется путем объединения локальных киберсред. На базе академической киберсреды формируется цифровая академическая экосистема, в рамках которой функционируют все участники – физические и юридические лица, которые являются представителями академического сообщества (рис. 1). Единая академическая киберсреда обеспечивает комплексную информатизацию и автоматизацию академического сообщества и образовательного процесса.

Одной из важнейших проблем, возникающих при формировании единого академического киберпространства, является возможность комплексирования распределенного программного обеспечения киберсреды из отдельных независимых модулей различного уровня разукрупнения. Наиболее рациональным решением является создание модулей, имеющих микросервисную архитектуру, с единой службой аутентификации.

Одним из базовых принципов построения единой киберсреды является агентность. В роли агента могут выступать физические лица, группы пользова-

телей, а также любые техногенные объекты. Выступая в роли цифрового двойника, агенты содержат в себе минимально необходимую информацию для работы с микросервисами академической киберсреды.

Доверительное взаимодействие агентов и микросервисов в рамках академической киберсреды определяется с помощью механизма аутентификации и использования доверенного сертификата, предоставленного ядром среды. Ядро академической киберсреды состоит из трёх основных микросервисов:

– аутентификации;
– менеджера связей между агентами;
– информационных профилей агентов.

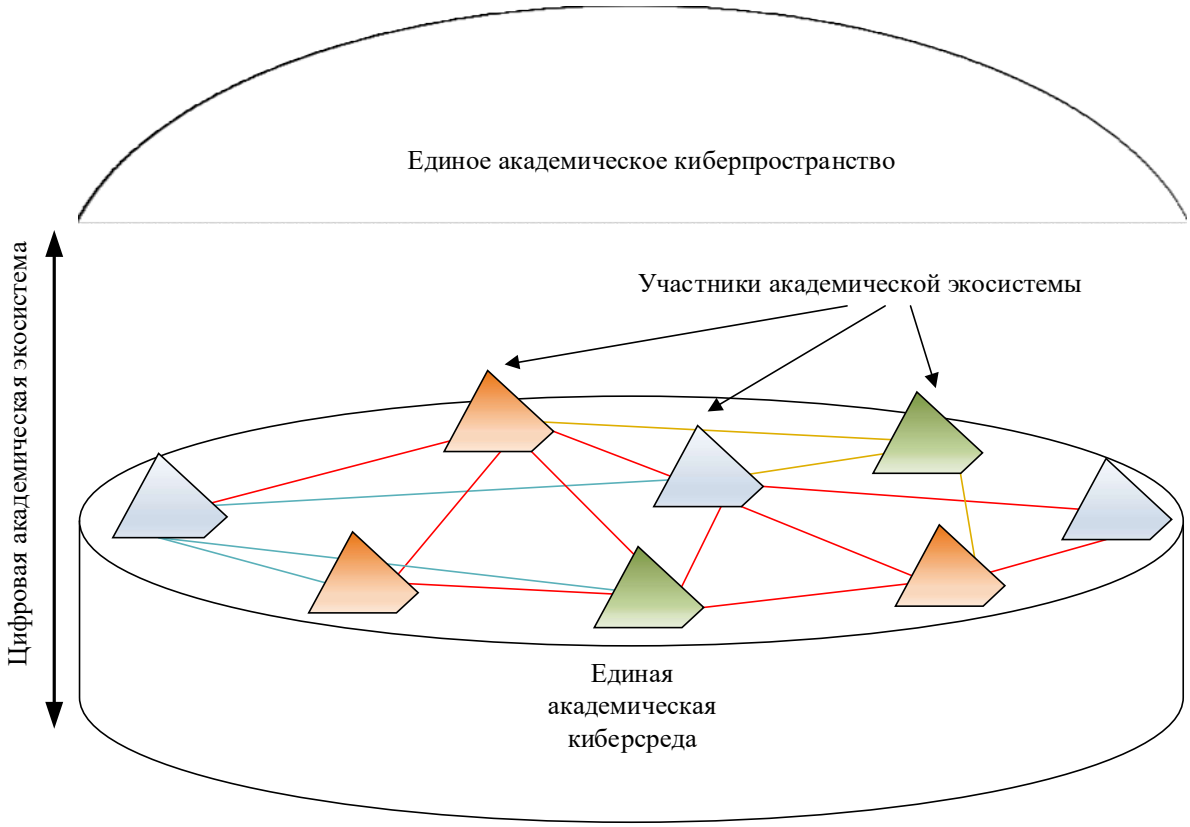


Рис. 1. Концепция единой академической киберсреды и цифровой академической экосистемы, формируемой на ее основе

В процессе регистрации агента в единой академической киберсреде информация о новом агенте фиксируется в трех микросервисах: менеджере связей, сервере аутентификации и в службе информационных профилей (рис. 2). При использовании киберсреды каждый микросервис относящийся к ядру системы вызывается другими микросервисами только в случае необходимости получения информации об агенте или отношениях между агентами, так как все микросервисы являются максимально независимыми друг от друга. Микросер-

висы, не входящие в ядро киберсреды, используют сертификацию как для взаимодействия с ядром, так и для взаимодействия друг с другом во избежане несанкционированного доступа. Микросервисы, работающие автономно от ядра, могут предоставлять свои данные напрямую. Сервисы, для функционирования которых требуются данные об агентах, могут обращаться к ядру киберсреды и получать соответствующие данные, в случае если они имеют необходимые права.

На рис. 2 представлен пример взаимодействия микросервисов. При обращении к сервисам тестирования и анализа переходов по гиперссылкам академической киберсреды запрашиваются данные из ядра системы, включая менеджер связей и сервис управления информационными профилями. В работе данных микросервисов такая информация, полученная из ядра киберсреды, необходима для идентификации пользователя с целью аналитики посещенных им ресурсов и подборке тестовых заданий для конкретного физического лица. Аналитика переходов содержит в себе сведения о любых посещенных ресурсах как за пределами академической киберсреды, так и внутри её. Микросервис с банком тестовых заданий использует менеджер связей и информацию о пользователе с целью сохранения результатов тестирования и локальной аналитикой ответов на конкретные задания агентами физических лиц с целью подбора индивидуальных траекторий обучения. Микросервис с новостной лентой также использует сервисы ядра, однако цель подобных связей заключается в том, чтобы предложить агенту информационные ресурсы, которые могут быть представлять для него интерес. Данный сервис формирует подборку ресурсов с учетом информации, полученной от микросервиса аналитики и переходов по гиперссылкам в киберсреде.

Представленная модель комплексирования академической киберсреды из отдельных сервисов различных уровней разукрупнения обеспечивает возможность формирования единой академической киберсреды из модулей, созданных независимыми разработчиками. Аналогичный подход, примененный для комплексирования магистрально-модульных радиоэлектронных систем, хорошо зарекомендовал себя в управлении сложностью [8].

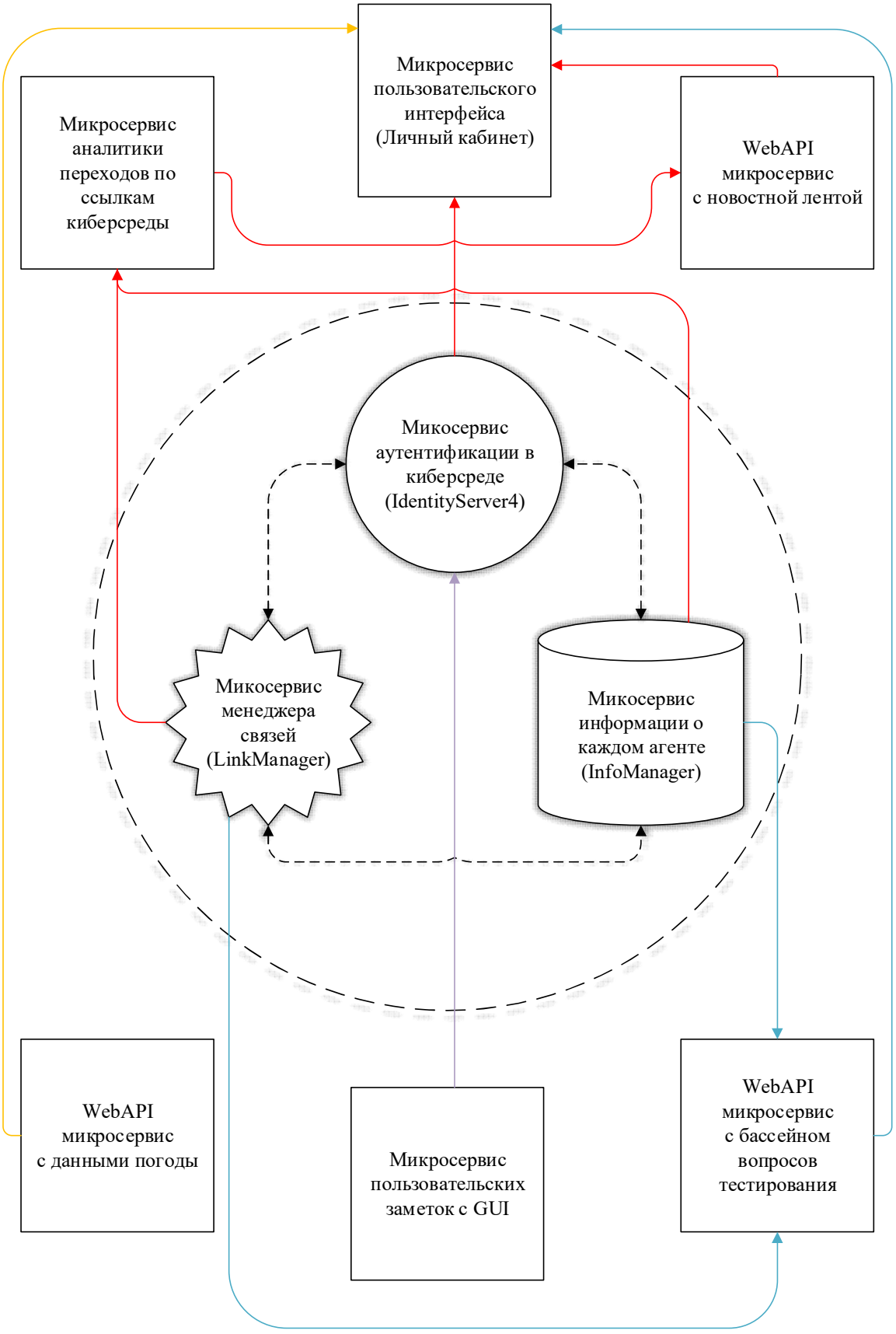


Рис. 2. Модель комплексирования киберсреды и взаимодействия микросервисов с ядром киберсреды и друг с другом

Список используемых источников

1. Поначугин А. В., Лапыгин Ю. Н. Цифровые образовательные ресурсы ВУЗа: проектирование, анализ и экспертиза // Вестник Мининского университета. 2019. Том 7, № 2. С. 5–8.

2. Кривопалова И. В. Смешанное обучение как инновационный путь модернизации образовательной сферы // Вестник ТГУ. 2013. Т. 18. Вып. 1. С. 6–13.

3. Корякин Ю. В. Новая парадигма образования // Вестник Томского государственного университета. 2009. № 39. URL: http://cyberleninka.ru/ article/n/novaya-paradigma-obrazovaniya (дата обращения 29.03.2021).

4. Sandhu, G. The Role of Academic Libraries in the Digital Transformation of the Universities // 2018 5th International Symposium on Emerging Trends and Technologies in Libraries and Information Services (ETTLIS), Noida, India, 2018. Pp. 292–296.

5. Горбунов А. С. Личность и цифровые технологии в информационном массовом обществе // Вестник Московского государственного областного университета. Серия: Философские науки. 2018. № 4. С. 8–16.

6. Краснова Г. А., Можаева Г. В. Электронное образование в эпоху цифровой трансформации: научное издание. Томск: Издательский Дом Томского государственного университета, 2019. 200 с.

7. Акимов С. В., Верхова Г. В., Меткин Н. П. Теоретические основы CALS : монография / СПбГУТ. СПб., 2018. 263 с.

8. Шубарев В. А., Меткин Н. П., Зверев В. Н. Магистрально-модульное построение РЭС – стратегическое направление радиоэлектронного приборостроения // Электроника: наука, технология, бизнес. 2008. Спец. вып. С. 20–23.

УДК 004.056.5:342.84
ГРНТИ 81.93.29

ПРОТОТИП СИСТЕМЫ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ НА ОСНОВЕ ПРОТОКОЛА С РАЗДЕЛЕНИЕМ СЕКРЕТА И АКТИВНЫХ УСТРОЙСТВ АУТЕНТИФИКАЦИИ

А. С. Вишневский, Д. О. Маркин

Академия Федеральной службы охраны Российской Федерации

В статье приводится предложение по реализации прототипа системы электронного голосования на основе протокола с разделением секрета и активных устройств аутентификации. Приведены основные требования, выдвигаемые к системам электронного голосования Разработана структурная схема основных компонентов системы электронного голосования. Сформулированы выводы в отношении развития данной технологий

блокчейн, обезличенная обработка персональных данных, разделение секрета, электронное голосование.

Введение

Современный уровень развития информационных систем и технологий, а также избранный путь на цифровизацию экономики и государственного управления затрагивает и достаточно специфические и важные права каждого гражданина на свободное участие в выборах органов государственного управления. Анализ руководящих документов в данной области [1, 2] показывает, что нормативно-правовая база постепенно готовится, а ряд имеющихся программных продуктов и проводимых в России экспериментов [3, 4] указывает на то, что данному вопросу уделяется много внимания. Существует также и ряд программных продуктов, реализующих функции электронного голосования [5, 6], а также их публичная критика [7, 8].

Таким образом, можно сделать вывод, что современные реалии требуют наличия эффективной защищенной системы электронного голосования, которой в настоящее время пока проходит стадию апробации и исследования эффективности. В связи с этим, актуальной задачей является задача разработки защищенной системы электронного голосования с применением ряда технологий защиты, позволяющих обеспечить информационную безопасность процедуры голосования.

Электронное голосование посредством удаленного доступа небезопасно пока не реализован протокол, который одновременно предохраняет от мошенничества, несанкционированного доступа к результатам голосования, а также не защищает тайну личности и тайну голосования. Идеальный протокол должен обладать, поменьше мере, следующими шестью свойствами:

Голосовать могут только те, кто имеет на это право.

Каждый может голосовать не более одного раза.

Никто не может узнать, за кого проголосовал конкретный избиратель.

Никто не может проголосовать вместо другого.

Никто не может тайно изменит чей-то голос.

Каждый голосующий может проверить, что его голос учитывался при подведении итогов голосования.

Кроме того, для некоторых схем голосования может понадобиться следующие требования:

Каждый знает, кто голосовал, а кто нет.

Для удовлетворения данных требований необходимо объединить следующие компоненты и технологии:

Блокчейн – как технология, позволяющая хранить хронологическую последовательность данных, защищенную от модификации криптографическими средствами защиты.

Разделение секрета – как технология, позволяющая обеспечить тайну голосования и нарушение целостности результатов голосования.

Аутентификация средствами аппаратных идентификаторов – как технология надежной проверки подлинности избирателей.

Обезличенная обработка персональных данных – на базе технологии разделения секрета.

Авторизация пользователей – является функцией определения прав доступа к ресурсам и управления этим доступом.

Предложение решения данной задачи

Для реализации данных требований предлагается следующее решение:

Шаг 1. Клиент авторизуется и запрашивает бюллетень.

Шаг 2. Сервер проверяет, имеет ли право голоса данный клиент. Если имеет, то он записывает данные пользователя и выдает бюллетень. Список пользователей, имеющих право голосовать, публикуется заранее, а также по итогам голосования публикуется список пользователей, которые приняли участие в голосовании.

Шаг 3. Сервер набирает пул запросов от клиентов с определенным промежутком времени (для того чтобы в серии было различное количество бюллетеней, а конкретное количество бюллетеней в серии, известно только серверу и, в последствии, центру распределения бюллетеней для предотвращения фальсификации с внешней стороны) и выдаются так называемые серии (при этом сервер знает номера бюллетеней и их количество в каждой серии, а также кому выданы бюллетени, но при этом какая бюллетень распределена каждому пользователю неизвестно).

Шаг 4. Сервер распределения бюллетеней раздает, сгенерированные сервером, бюллетени случайным образом пользователям оставивших заявки.

Шаг 5. На клиенте к бюллетеням пользователя добавляется свой идентификатор (квитанция) и шифруется своим закрытым ключом (который есть только у пользователя). Данный ключ генерируется при помощи случайного нажатия клавиш и вращения манипулятора типа мышь. Таким образом пользователь по номеру бюллетеня может узнать правильно ли учтен его голос.

Шаг 6. В случае желания пользователя изменить свой голос, он отправляет запрос на сервер о желании отозвать свой голос с указанием номера бюллетеня.

Шаг 7. Сервер проверяет наличие данного бюллетеня, в случае реального нахождения данного бюллетеня сервер запрашивает закрытый ключ к квитанции.

Шаг 8. При правильном расшифровании квитанции сервер сверяет идентификатор в квитанции с идентификатором пользователя, отправившего запрос на отзыв голоса.

Шаг 9. В случае соответствия данный голос отзывается, и пользователь производит голосования повторно. При этом генерируя новый закрытый ключ. Возможность переголосовать предоставляется пользователю один раз в сутки для избегания атак типа *DDoS*.

На рис. представлена структурная схема реализации данной системы.

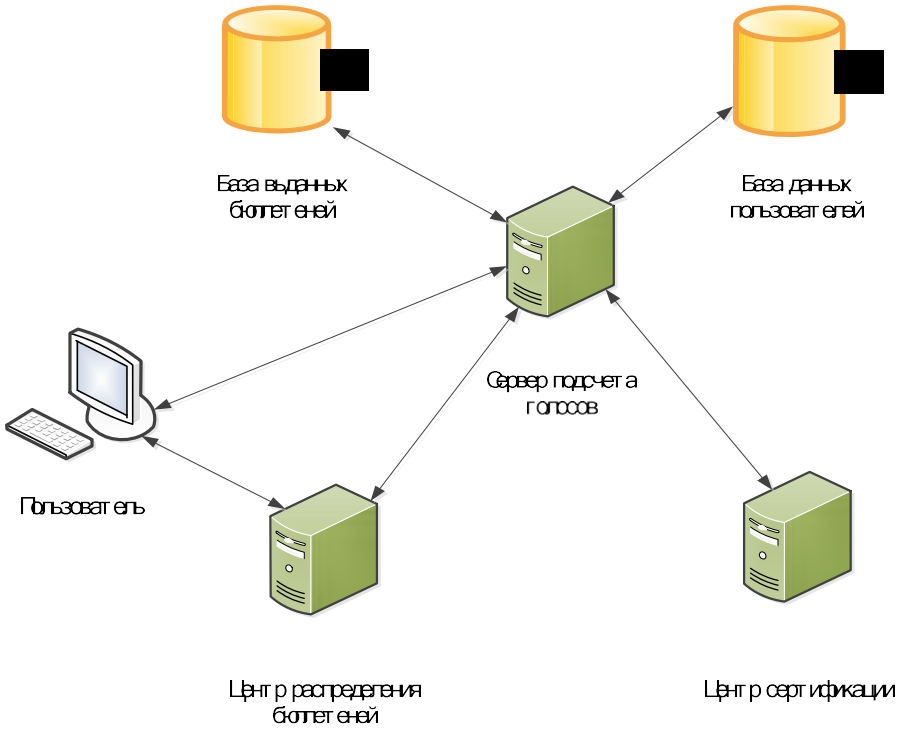


Рис. Структурная схема прототипа системы электронного голосования

В целях обеспечения вопросов защиты информации, защиты от несанкционированного доступа, тайны голосования может быть реализованы следующий протокол защиты.

Инициализация системы. На данном этапе выполняются следующие операции:

– выработка ключевой пары валидатора для проверки и выдачи слепой подписи (СП). Применяется протокол *RSA* с длиной ключа 4 096 бит;

– выработка общего открытого ключа шифрования. Применяются протокол *DKG Pedersen* 91 для распределенной выработки ключа и протокол разделения ключа Шамира.

Предоставление доступа к бюллетеню. На данном этапе выполняются следующие операции:

– выработка ключевой пары электронной подписи (ЭП) по ГОСТ Р 34.10–2012;

– выработка СП для маскирования открытого ключа необходимого для получения права голосования. Применяется алгоритм *RSA*.

– Заполнение и отправка бюллетеня. На данном этапе выполняются следующие операции:

– шифрование бюллетеня. Применяется схема Эль-Гамаля реализованная на эллиптических кривых;

− доказательство достоверности содержимого бюллетеня. Применяется *Disjunctive Chaum-Pedersen range proof* (доказательство с нулевым разглашением);

− ЭП зашифрованного бюллетеня по ГОСТ Р 34.10–2012.

Подсчет итогов. На данном этапе выполняются следующие операции:

− гомоморфное сложение бюллетеней. Применяется схема Эль-Гамаля реализованная на эллиптических кривых;

− частичное расшифрование итогового суммированного бюллетеня. Применяются части закрытого ключа участников, контролирующих отдельные ноды;

− в избирательной комиссии осуществляется сборка закрытого ключа и частичное расшифрование итогового суммированного бюллетеня. Применяется собранный ключ;

− производится окончательное суммирование голосов и получение итогов голосования;

− доказательство корректности итогов голосования. Применяется *Chaum-Pedersen proof* (выработка и проверка доказательства с нулевым разглашением).

Аудит. На данном этапе может быть выполнена проверка корректности на каждом шаге.

Представленный криптографический протокол системы дистанционного электронного голосования позволяет удовлетворить предъявляемые к системам требования электронного голосования.

Выводы

Электронное голосование направлено на увеличение числа участников, снижение затрат на проведение выборов и повышение точности результатов. В этой статье описаны требования и реализация специального типа систем электронного голосования, системы удаленного онлайн-голосования, подходящей для университетов, где студенты могут отдавать свои голоса в любое время, в любом месте и с использованием стационарных и мобильных электронных устройств, включая персональные компьютеры, персональные цифровые помощники, умные и обычные телефоны.

Список используемых источников

1. Российская Федерация. Законы. Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации : федер. закон от 12.06.2002 № 67-ФЗ : [принят Гос. Думой 22 мая 2002 г. : одобр. Советом Федерации 29 мая 2002 г.] // Официальный интернет-портал правовой информации : сайт. – в ред. Федерального закона от 31.07.2020 № 267-ФЗ. Электрон. дан. 2005–2020. URL: http://publication.pravo.gov.ru/Document/View/0001201807030055 (дата обращения 08.12.2020).

2. Российская Федерация. Законы. О внесении изменений в отдельные законодательные акты Российской Федерации : федер. закон от 23.05.2020 № 154-ФЗ : [принят Гос. Думой 13 мая 2020 г. : одобр. Советом Федерации 20 мая 2020 г.] // Официальный интернет-портал правовой информации : сайт. Электрон. дан. 2005–2020. URL: http://publication.pravo.gov.ru/Document/View/0001202005230002 (дата обращения 08.12.2020).

3. Российская Федерация. Законы. О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» : федер. закон от 24.04.2020 № 123-ФЗ : [принят Гос. Думой 14 апреля 2020 г. : одобр. Советом Федерации 17 апреля 2020 г.] // Официальный интернет-портал правовой информации : сайт. Электрон. дан. 2005–2020. URL: http://publication.pravo.gov.ru/ Document/View/0001202004240030. (дата обращения 08.12.2020).

4. Российская Федерация. Законы. О проведении эксперимента по организации и осуществлению дистанционного электронного голосования в городе федерального значения Москве : федер. закон от 23.05.2020 № 152-ФЗ : [принят Гос. Думой 13 мая 2020 г. : одобр. Советом Федерации 20 мая 2020 г.] // Официальный интернет-портал правовой информации : сайт. Электрон. дан. 2005–2020. URL: http://publication.pravo.gov.ru/ Document/View/0001202005230001 (дата обращения 08.12.2020).

5. Платформа для проведения электронного голосования на базе технологий распределенных реестров : свидетельство о государственной регистрации программы для ЭВМ № 2020612936 Российская Федерация / В. Н. Петрунин, Д. А. Кириллов, М. А. Макаров, О. О. Якушкин, В. В. Корхов; правообладатель ФГБОУ ВО "Санкт-Петербургский государственный университет". – № 2019663251 ; заявл. 24.10.2019; опубл. 06.03.2020; зарегистрировано в Реестре программ для ЭВМ 06.03.2020 г. – Бюл. № 3.

6. Система дистанционного электронного голосования компании "Ростелеком" / ПАО Ростелеком // ПАО Ростелеком : сайт. Электрон. дан. …–2020. URL: https://www.company.rt.ru/projects/elections/about.php (дата обращения: 23.03.2021).

7. Обсуждение системы голосования, разработанной ДИТ Москвы / nnseva // Блог "Хабр" : сайт. Электрон. дан. 2005–2020. URL: https://habr.com/ru/post/507640/ (дата обращения: 08.12.2020).

8. Обзор системы дистанционного электронного голосования ЦИК РФ / RTteam // Блог "Хабр" : сайт. Электрон. дан. 2005–2020. URL: https://habr.com/ru/company/rostelecom/ blog/518090/ (дата обращения: 23.03.2021).

УДК 004.051
ГРНТИ 50.41.21

ВЛИЯНИЕ ДИСТРИБУТИВОВ LINUX ДЛЯ МИКРОКОМПЬЮТЕРА RASPBERRY PI НА ПРОИЗВОДИТЕЛЬНОСТЬ СУБД SQLITE

М. В. Владыкин, В. В. Громов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Важной частью разработки программного обеспечения является реализация работы с базами данных. При этом, требуется обеспечить минимальную задержку обновления значений в базах данных. Также при реализации графического интерфейса пользователя, необходимо обеспечить достаточную производительность, чтобы пользователь не испытывал дискомфорт при работе с программой. В статье изучается степень влияния наличия интерфейса пользователя в операционной системе на работу СУБД SQLite на примере одноплатного компьютера семейства Raspberry Pi.

базы данных, система управления базами данных, графический интерфейс пользователя, SQL, SQLite, Linux, Raspberry Pi.

Семейство одноплатных компьютеров Raspberry Pi является отличным примером того, что современные персональные компьютеры можно реализовать в миниатюрном корпусе. При этом, современные версии данных плат могут запускать полноценную операционную систему Linux даже с графическим окружением, что позволяет их использовать для проектирования полноценных информационных систем, несмотря на малую вычислительную мощность данных плат.

Проектирование современных информационных систем для конечного пользователя нуждается в создании GUI или, используя русскоязычный термин, графического интерфейса пользователя. GUI позволяет предоставить пользователю простой интерфейс взаимодействия с функционалом программы. Такой тип взаимодействия проще воспринять человеку, чем текстовый режим работы программы. Внедрение GUI уменьшает время отклика, количество ошибок и повышает оценку удовлетворенности пользователя программы [1].

Второй немаловажной частью современных информационных систем является системы управления базами данных или СУБД [2, 3]. СУБД позволяет создавать программы, где хранение, чтение и запись данных организовано с помощью базы данных. При использовании СУБД программист не тратит время на реализацию функций работы с данными, а пользуется готовыми функциями, что ускоряет процесс разработки программного обеспечения.

При малой вычислительной мощности плат Raspberry Pi в сравнении с персональными компьютерами, построенными на x86 архитектуре, от разработчиков программного кода требуется обеспечить эффективное использование вычислительных ресурсов.

Этими причинами обусловлено исследование влияния наличия графического окружения на быстродействие взаимодействия программ с СУБД на примере встраиваемой СУБД SQLite.

В ходе исследования было проведено тестирование программ, которые записывают данные в файл базы данных с помощью API SQLite. Тестовые программы были написаны с помощью языков программирования C++ и Python. В качестве компилятора для программы на языке C++ был использован GCC версии 8.3.0. Интерпретатор для языка Python был использован версии 3.7.3. Библиотека libsqlite3-dev для языка C++, использовалась версии 3.27.2-3.

Программы тестировались на плате Raspberry Pi model 3B+. В качестве накопителя была использована MicroSD карта-памяти компании SanDisk, модель SanDisk Ultra PLUS объемом 32 ГБ, скоростью записи 15 МБ/с и скоростью чтения 48 МБ/с.

Для исследования использовались два дистрибутива для данной модели платы – Raspberry Pi OS и Raspberry Pi OS Lite. В Raspberry Pi OS реализовано графическое окружение, а Raspberry Pi OS Lite нет.

Исследование представляет собой выполнение 100 SQL-запросов на запись данных в файл базы данных, с помощью API-SQLite. Время выполнения запросов измеряется с помощью стандартных функций языков программирования. Усредненные значения результатов измерений представлены и в таблице и их сравнение на рис.

ТАБЛИЦА. Результаты измерений времени выполнения запросов

	ОС без GUI		ОС с GUI		Единица измерений
Язык программирования	C++	Python	C++	Python	
Число повторений	100				
Среднее значение времени выполнения программы	3,42	18,24	3,49	20,40	мс
Отклонение значений	0,11	3	0,16	3,44	мс
Отклонение значений в %	3,3	14,0	4,5	16,9	%

Результаты измерений, продемонстрированные в таблице показывают значительное преимущество в скорости работы программы, написанной на языке программирования C++, над программой, написанной над языком программи-

рования Python. Высокая скорость работы программы дополняется более низким отклонением значений от среднего, что обеспечивает большую предсказуемость времени обработки SQL запросов.

Также данные показывают практически полную независимость результатов работы программы, написанной на языке C++, в отличии от программы на Python, где работа программы обеспечивается интерпретатором, что объясняет существенные различия во времени исполнения и отклонении измерений от среднего значения.

Скорость работы программ доказывает, что даже при малых вычислительных мощностях платы Raspberry Pi model 3B+, данная плата позволяет реализовывать полноценные программы, которые постоянно обращаются к базам данных, однако, следует понимать, что данные могут существенно измениться при изменении MicroSD карты-памяти, как в большую, так и в меньшую сторону.

Рис. Сравнение измерений времени выполнения запросов

Анализ результатов позволяет сделать следующие выводы:

1) СУБД SQLite показала высокую скорость обработки запросов даже на плате Raspberry Pi model 3B+.

2) Наличие GUI в ОС для Raspberry Pi слабо влияет на конечную скорость обработки запросов СУБД SQLite, что позволяет использовать вычислительные ресурсы системы на реализацию полноценного GUI для разрабатываемых программ для Raspberry Pi.

3) Отклонение измерений также увеличивается незначительно. Это позволяет сохранить предсказуемость времени исполнения модуля программы, который работает с SQL запросами.

Список используемых источников

1. Staggers, Nancy; Kobus, David. Comparing Response Time, Errors, and Satisfaction Between Text-based and Graphical User Interfaces During Nursing Order Tasks // Journal of the American Medical Informatics Association Volume 7 Number 2 Mar / Apr 2000. Pp. 164–176.

2. Шаякбаров Н. Ф., Зорин Д. С. Анализ производительности систем управления базами данных при работе с большим объемом информации // Инженерный вестник Дона. 2015. № 2, Ч. 2. URL: http://ivdon.ru/uploads/article/pdf/IVD_82_shayakbarov.pdf_e69e73bceb.pdf (дата обращения: 10.03.2021).

3. Тест встраиваемых БД // Журнал Хакер. 2007. URL: https://xakep.ru/2007/06/25/38720/ (дата обращения 10.03.2021).

УДК 004.051
ГРНТИ 50.41.21

ОПТИМИЗАЦИЯ РАБОТЫ API СУБД SQLITE НА МИКРОКОМПЬЮТЕРЕ RASPBERRY PI

М. В. Владыкин, В. В. Громов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Важной частью разработки программного обеспечения является реализация работы с базами данных. При этом, при малых вычислительных возможностях системы может потребоваться внедрение оптимизаций в код программы, чтобы снизить задержки выполнения SQL запросов. В статье демонстрируются рабочие методы оптимизации работы с API СУБД SQLite на примере одноплатного компьютера семейства Raspberry Pi и языка программирования C++.

оптимизация, базы данных, система управления базами данных, API, C/C++, SQL, SQLite, Linux, Raspberry Pi.

Проектирование современных информационных систем требует реализации системы хранения и работы с данными, в качестве которых, в основном, используют системы управления базами данных или СУБД. Эти СУБД являются уже готовыми разработками, взаимодействие с которыми необходимо реализовать в разрабатываемом программном обеспечении. Отличным примером СУБД является SQLite, которая показывает отличную производительность при

работе с базами данных. На высокопроизводительном компьютере эти показатели не превышают показателей в 0,3 секунды [1, 2].

Однако, если разрабатываемый проект нацелен на не столь высокопроизводительную платформу, например, одноплатный компьютер Raspberry Pi, то данный показатель может существенно возрасти, особенно, если использовать флеш-память с низкими скоростями записи и чтения. Поэтому, если возможно, то необходимо оптимизировать программный код, чтобы получить более быстрый отклик при работе с базой данных.

В ходе исследования возможностей ускорить работу выполнения запроса по записи данных в базу данных, было найдено решение по оптимизации программного кода на языке программирования C++, взаимодействующей с СУБД SQLite посредством API SQLite, для одноплатного компьютера Raspberry Pi model 3B+ с накопителем компании SanDisk, модель SanDisk Ultra PLUS объемом 32 ГБ, скоростью записи 15 МБ/с и скоростью чтения 48 МБ/с.

Сначала рассмотрим, как с помощью API SQLite выполняются запросы к базе данных. Для этого в API SQLite для языков программирования C/C++ реализована функция – sqlite3_exec(sqlite3*, const char *sql, int (*callback)(void*,int,char**,char**), void *, char **errmsg) [3]. В качестве аргументов она принимает:

1) Указатель на открытую базу данных – sqlite3*;
2) Строку с SQL запросом – const char *sql;
3) Указатель на функцию обратного вызова – int (*callback)(void*,int,char**,char**);
4) Указатель на первый аргумент для функции обратного вызова – void *;
5) Указатель на строку, куда запишется ошибка выполнения – char **errmsg.

Результаты тестирования данной функции при записи в базу данных представлены в таблице 1.

ТАБЛИЦА 1. Результаты измерений времени выполнения запросов с помощью функции sqlite3_exec

	Файловая БД	БД в ОЗУ
Число запросов	100	
Среднее значение времени выполнения запросов	0,178 с	15,04 мс
Отклонение значений	0,004 с	0,36 мс
Отклонение значений, %	2,3	2,4

Для повышения быстродействия выполнения запросов предлагается использовать следующие оптимизации:

После открытия базы данных, необходимо выполнить следующие запросы:

1) PRAGMA synchronous = OFF – данный запрос позволяет отключить дублирование данных;

2) PRAGMA journal_mode = MEMORY – данный запрос позволяет хранить журнал базы данных в оперативной памяти;

3) PRAGMA temp_store = MEMORY – данный запрос позволяет хранить временные таблицы в оперативной памяти;

4) PRAGMA page_size = 8192 – данный запрос позволяет установить размер страницы для базы данных.

Далее все маленькие транзакции следует объединять в одну большую транзакцию с помощью команд – BEGIN TRANSACTION и COMMIT.

Каждый отдельный запрос необходимо обрабатывать без использования функции sqlite3_exec, так как это – объединенный интерфейс над несколькими функциями, который замедляет скорость выполнения отдельных функций (команд). Вместо этого предлагается использовать функции:

1) sqlite3_prepare() – для подготовки указателя на запрос;

2) Семейство функций sqlite3_bind() – для добавления значений переменных к запросу;

3) sqlite3_step() – для выполнения запроса;

4) sqlite3_finalize() – для уничтожения указателя на запрос.

В таблице 2 представлены данные тестирования выполнения запросов записи в базу данных, после внедрения предлагаемых оптимизаций.

ТАБЛИЦА 2. Результаты измерений времени выполнения запросов после внедрения оптимизаций

	Файловая БД	БД в ОЗУ
Число запросов	100	
Среднее значение времени выполнения запроса	0,00342 с	2,81 мс
Отклонение значений	0,0001 с	0,02 мс
Отклонение значений в %	3,3	0,7

Из полученных данных можно сделать вывод, что среднее время выполнения запросов уменьшилось в 52 раза, в случае использования файловой базы данных. При этом, небольшое увеличение отклонения значений может быть объяснено неточностью стандартных функций для измерения времени выполнения программы. В случае использования базы данных в оперативной памяти, оптимизации позволяют ускорить выполнение запросов, в среднем, в 5,3 раза, что при размерности в миллисекунды существенно. Все сравнительные данные

для файловой базы данных представлены в виде диаграммы на рис. 1. Сравнительные данные для базы данных в оперативной памяти представлены на рис. 2.

Рис. 1. Сравнение измерений времени выполнения запросов в файловую БД

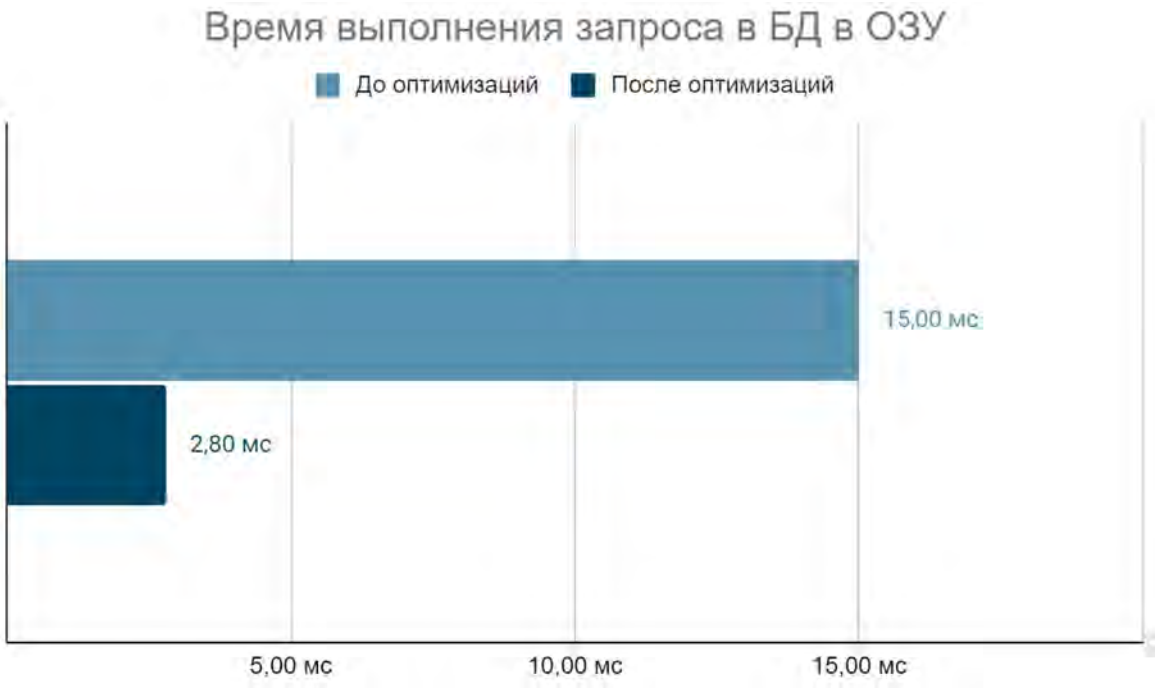


Рис. 2. Сравнение измерений времени выполнения запросов в БД в ОЗУ

В данной работе продемонстрированы результаты оптимизаций работы с API SQLite на языке программирования C++, которые существенно снизили время выполнения запросов к базе данных.

Список используемых источников

1. Шаякбаров Н. Ф., Зорин Д. С. Анализ производительности систем управления базами данных при работе с большим объемом информации // Инженерный вестник Дона. 2015. № 2, Ч. 2. URL: http://ivdon.ru/uploads/article/pdf/IVD_82_shayakbarov.pdf_e69e73bceb.pdf (дата обращения 10.03.2021).
2. Тест встраиваемых БД // Журнал Хакер. 2007. URL: https://xakep.ru/2007/06/25/38720/ (дата обращения 10.03.2021).
3. C-language Interface Specification for SQLite. URL: https://sqlite.org/capi3ref.html (дата обращения 10.03.2021).

УДК 57.024; 004.514
ГРНТИ 34.03.23

ФОРМИРОВАНИЕ ПОЛЬЗОВАТЕЛЬСКОГО ОПЫТА НА ОСНОВЕ ОБУЧАЮЩЕГО ФАКТОРА ВСЛЕДСТВИЕ ОШИБОЧНЫХ ДЕЙСТВИЙ

Д. В. Волошинов, А. В. Генчева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена рассмотрению процесса формирования пользовательского опыта на основе обучающего фактора при совершении ошибочных действий с точки зрения когнитивной психологии, в частности последовательного применения разных типов памяти: сенсорной, рабочей и долговременной. Воздействующим стимулом выступает эмоциональное воздействие отрицательного и положительного характера. Предусматривается ограничение мозговой активности. Эффективность формирования пользовательского опыта при целевом использовании вследствие обучения определена в результате проведенного юзабилити-тестирования раздела администрирования лабораторной подсистемы медицинской информационной системы «Ариадна».

пользовательский опыт, когнитивная психология, сенсорная память, рабочая память, долговременная память, гипоталамус.

Негативное проявление пользовательских ошибочных действий проявляется в отказе от использования продукта и значительной потере временных ресурсов. Однако в стрессовом состоянии проблемные ситуации формируют пользовательский опыт, характеризующий восприятие и ответные действия пользователя, возникающие в результате текущего или предстоящего использования системы, в ускоренном режиме [1]. Биологический смысл приобретенных рефлексов состоит в прогнозировании поведения системы и упрощении

взаимодействия, что повышает эффективность решения текущих задач сотрудников. Ожидаемое использование влияет на удовлетворенность фактического применения [2]. В процессе формирования определяется совокупность ощущений от взаимодействия с интерфейсом, включая физическое и психологическое состояние пользователя, которое является результатом предыдущего опыта, привычек, навыков и условия использования.

Реагирование организма человека при ошибочных действиях раскрывает область нейробиологии – когнитивная психология, учитывающая процессы мозговой активности, необходимые для запоминания, восприятия, реагирования и анализа пользовательских отвлечений.

Формирование надежного пользовательского опыта происходит при последовательном использовании разных типов памяти: сенсорной или знаковой, рабочей и долговременной [3]. Восприятие избыточных раздражителей осуществляется с помощью всех органов чувств. Процесс формирования пользовательского опыта запускает сильно действующий стимул, в частности стрессовое состояние. Центром страха выступает гипоталамус, расположенный в промежуточном мозге [4]. В течение доли секунд бессознательно действует сенсорная память пользователя, сохраняя данные, попадающие на сетчатку глаза.

Следующий этап осуществляется сосредоточением внимания на воздействующем стимуле до момента перемещения в рабочую память, которая длится тридцать секунд и имеет ограниченную способность хранения информации. Задействованный адреналин ускоряет действие с целью поиска выхода из проблемной ситуации. Подобный процесс сохранения важной информации в процессе формирования пользовательского опыта в когнитивной психологии является долговременной потенциацией. Достижение данных по своду гиппокампа височной доли, пучка белого вещества из аксонов, через таламус в поясную извилину или круг Пейпеза выполняет функцию формирования рабочей памяти в течение дня [4]. При воздействии сильного стимула, химического вещества дофамина, определяющего удовольствие, выбиваются магниевые пробки. Важная найденная информация рабочей памяти сохраняется и переходит в следующую стадию формирования опыта, а лишняя – стирается во время сна во избежание переполнения данных в гиппокампе. Стоит отметить, что лучшее запоминание данных происходит при разбиении на значимые группы по три или четыре элемента. Дальнейшее достоверное сохранение зависит от полного удаления лишних данных из рабочей памяти.

Рабочая память динамична. Различная сенсорная информация располагается в совокупности с долговременными воспоминаниями или семантическими понятиями. Ключевое ограничение проявляется в случае размещения новых данных: по причине полного заполнения сохранение в рабочей памяти доступно только при замещении имеющейся информации или полном стирании

по истечении тридцати секунд без проявления активных действий для последующей записи в долговременную память [3].

На третьем этапе неоднократного повторения задействована глутаминовая кислота как главный возбуждающий медиатор мозга, которая влияет на формирование обнаруженного решения в долговременной памяти. Пользовательский опыт впоследствии совершения ошибочного действия сформирован. В результате при образовании канала передачи информации участвуют зрительный центр, промежуточные нейроны коры, центры положительного подкрепления и запускающие реакцию.

Чем дольше обрабатывается проблемная ситуация, тем большее напряжение, называемое потенциалами действия, пользователь направляет через нейронную сеть, в которой образуются синапсы и толстые дендриды, размещаемые в конце ветви [3]. Подобный процесс приводит к эффективной активации точных воспоминаний о найденном ранее решении.

При дальнейшем обращении к похожей проблемной ситуации распознавание новых необработанных образов осуществляется с помощью задействованной поясной извилины, сравнивающей поступающую информацию с записанной ранее в долговременной памяти.

В процессе проведения юзабилити-тестирования, направленного на обнаружение возможных ошибочных действий пользователя при взаимодействии с интерфейсом раздела администрирования медицинской информационной системы «Ариадна», для получения достоверных данных применяется оборудование отслеживания взгляда «Tobii Eye Tracker 4C». В результате обнаружены фиксации времени запуска сенсорной и кратковременной памяти при ошибочном вводе данных в диапазон референтных интервалов, соответствующие значениям в когнитивной психологии. Повышение эффективности использования продукта на основе долговременной памяти заключается в сформированном предыдущем пользовательском опыте при повторном обращении к похожей проблемной ситуации. Впоследствии сотрудники выполнили задачу на двенадцать секунд быстрее, чем при первичном ознакомлении с функциональными особенностями медицинской информационной системы, что доказывает положительный аспект ошибочных действий.

Список используемых источников

1. ГОСТ Р ИСО 9241-210 – 2012. Эргономика взаимодействия человек-система. Человеко-ориентированное проектирование интерактивных систем: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 29.11.2012 N 1290-ст. М.: Стандартинформ, 2013. 31 с.

2. ISO 9241-11:2008. Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts. URL: https://www.iso.org/obp/ui/ #iso:std:iso:9241:-11:ed-2:v1:en (дата обращения 26.12.2021).

3. David C. Evans. Bottlenecks: Aligning UX Design with User Psychollogy. M.: Apress, 2017. 260 с.

4. Дубынин В. А. Нейрофизиология поведения // Открытое образование. Московский государственный университет имени М. В. Ломоносова, 2020.

УДК 004.94
ГРНТИ 20.01.07

РАЗРАБОТКА МОДЕЛИ ИС ДЛЯ ПОДДЕРЖКИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА В УСЛОВИЯХ ПРИМЕНЕНИЯ СРЕДСТВ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

Д. В. Волошинов, А. М. Кравченко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Технология дополненной реальности в образовании все активнее заполняет область образования в большинстве стран. Электронные книги, интерактивные доски, планшеты – все это помогает улучшить образовательный процесс и сделать его продуктивнее. Проблема и цель статьи – исследование перспектив технологий AR инновационного развития образовательных услуг в сфере геометрии. Актуальность проблематики обоснована быстрым развитием и внедрением информационно-коммуникационных технологий в различные области социальной деятельности, среди которых и образовательная сфера. В статье раскрывается понятие технологии AR и рассматривается влияние информационных технологий в образовании. Авторами уделяется внимание строению приложения дополненной реальности и алгоритму его работы.

дополненная реальность, образование, технологии, AR.

В настоящее время технологии виртуальной и дополненной реальности стали общедоступны. Стоимость очков и шлемов VR/AR реальности снизилась, и в том числе основная масса современной техники хорошо справляются с приложениями дополненной реальности. Таким образом, позволило расширить сферу использования технологии, сориентировав её в том числе и на образовательную среду.

Многие образовательные учреждения в современном мире уже применяют дополненную реальность на базовых учебных предметах, таких как физика, химия, астрономия, история и т. д. Принцип наглядности работает куда эффективнее, чем устаревшие способы – изучение материала по учебникам, просмотр изображений, видео и многое другое. Это, во-первых, увлекательнее, а во-вторых, наделяет более ясным пониманием о вещах, процессах и событиях.

Целью данного исследования является разработка прототипа вспомогательного инструмента для решения стереометрических задач в рамках когнитивно-визуального подхода к обучению геометрии.

Существует мнение, что мы постоянно окружены математикой, чувствуем ее присутствие в архитектуре, дизайне, искусстве, и прежде всего – в природе (ульи, раковины улиток и т. д.). С этим утверждением довольно сложно не согласиться, но, тем не менее, не каждый человек может видеть мир так, как математики. Возникает острая необходимость раздвигать границы с точки зрения того, что визуально доступно, а что нет. Соответственно появляется задача – сделать абстрактные вещи видимыми, чтобы каждый мог их лучше понять. Это похоже на человеческое воображение – создание изображений даже очень сложных предметов делает их намного проще для понимания.

Пространственное мышление позволяет быстрее изучить и решить задачи, особенно нестандартные или современные проблемы в математике. Не так давно стали замечать взаимосвязь между пространственным мышлением и обучением точным наукам. Особое внимание на пространственном мышлении способствует наглядности в сфере математики. Исследуя пространственную сторону рассматриваемого объекта, математика становится более понятной, завораживающей и подходящей современным задачам [1]. Усовершенствование пространственного мышления является насущной проблемой текущего математического образовательного процесса, которой ещё не уделяется подобающего интереса. К сожалению, традиционные методы обучения часто не позволяют адаптировать учащихся к изучению геометрии и не могут помочь им улучшить свои знания. Вот почему учителя все чаще обращаются к готовым 3D-визуализациям, которые позволяют им показать твердое тело с разных сторон. Однако учащимся по-прежнему трудно решать задачи, требующие от них развитых навыков пространственного мышления. Отсутствие взаимодействия с трехмерными объектами и необходимость выполнять так называемое мысленное вращение мешает их пониманию трехмерной геометрии. Это приводит к тому, что не только ученикам, но и многим учителям пространственная геометрия кажется абстрактной областью математики. Согласно словам изобретателя виртуального симулятора, Мортона Хейлинга [2], информатизация в области образования является одним из важнейших направлений, так как информационные технологии при грамотном их применении увеличивают эффективность образования.

Дополненная реальность – компьютерная технология, демонстрирующая пользователю окружающий мир с наложенными на него виртуальными предметами, что дает эффект пребывания в едином пространстве. Существует два основных принципа создания AR:

– на основе маркера;
– на основе координат пользователя [3].

Безмаркерные технологии нередко используются в мобильных устройствах с поддержкой всевозможных интегрированных датчиков. В данной статье рассматривается технология на базе применения маркеров.

Наглядным примером применения дополненной реальности в сфере геометрии служит приложение Construct3D – инструмент для создания трехмерных геометрических конструкций. Данное приложение работает с помощью шлемов виртуальной реальности и контроллеров, упрощающий трехмерную модель. Construct3D позволяет нескольким людям работать в одном месте и создавать всевозможные геометрические модели, которые накладываются на окружающий мир. Как работает данный инструмент показано на рис. 1 [4, 5].

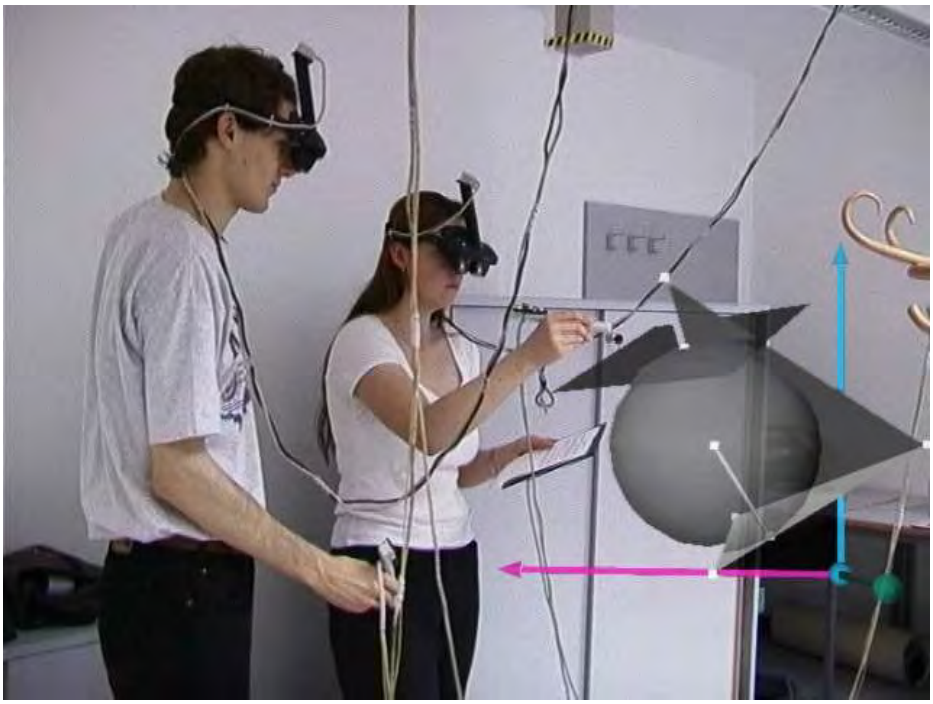


Рис. 1. Дополненная реальность в Construct 3D

Визуализация и совмещение цифровых и настоящих объектов предоставляет возможность нового способа решения задач в области стереометрии. После того, как проанализировав проблему решения школьниками задач пространственной геометрии и возможностей применения AR для визуализации, пришли к заключению, что применение этой технологии в данной области многообещающе. Было принято решение создать прототип приложения для мобильных устройств, так как они наиболее распространены и доступны.

У студента имеется распечатанный комплект задач по пространственной геометрии с маркерами (метками дополненной реальности). При запуске приложения на смартфоне должен включаться захват камеры. Пользователь наводит камеру на задачу так, чтобы маркер был в зоне видимости, на экране отображается соответствующий метке трехмерный объект, представляющий собой

визуализацию задания, например, изображает сечение пирамиды в соответствии с данными текущей задачи.

Далее представлен принцип работы приложения:

Рис. 2. Принцип работы приложения

Рис. 3. Пример интерфейса приложения

Выше представлен прототип приложения. В интерфейсе присутствует надпись, указывающая на номер задачи, и несколько кнопок – помощь, масштабирование и поворот. При нажатии на знак вопроса появляется подсказка в виде

формул по теме и ссылкой на сайт, где находятся решения с похожими задачами. Кнопки масштабирование и поворот дают возможность изменять фигуру в соответствии с их предназначением.

В настоящее время дополненная реальность (AR) становится все более распространенной и популярной в школах и классах. AR может повысить творческие способности и логический анализ учеников и студентов. Взаимодействие с виртуальными объектами через интерфейсы AR предоставляет учащимся все более интуитивно понятный и естественный способ взаимодействия с геометрическими телами.

Список используемых источников

1. Paying Attention to Spatial Reasoning: Support Document for Paying Attention to Mathematics Education. Ontario: Queen's Printer for Ontario, 2014. 27 p.

2. Технология дополненной реальности как современный метод обучения школьников. URL: https://rosuchebnik.ru/material/tekhnologiya-dopolnennoy-realnosti/

3. Благовещенский И. А., Демьянков Н. А. Технологии и алгоритмы для создания дополненной реальности // Моделирование и анализ информационных систем. 2013. Т. 20, No. 2. С. 129–138.

4. Construct3D – An Augmented Reality System for Mathematics and Geometry Education // Interactive Media Systems. URL: https://www.ims.tuwien.ac.at/projects/construct3d

5. Construct3D: A Virtual Reality Application for Mathematics and Geometry Education. URL: https://www.cg.tuwien.ac.at/research/vr/studierstube/construct3d/

6. Дополненная реальность в образовании. URL: https://virtualnyeochki.ru/stati/dopolnennaya-realnost-v-obrazovanii

УДК 004.056.55
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ СТЕГАНОГРАФИЧЕСКОГО МЕТОДА LSB С АДАПТИВНЫМ ПОИСКОМ ОБЛАСТЕЙ ВСТРАИВАНИЯ ДАННЫХ В РАСТРОВЫХ ГРАФИЧЕСКИХ КОНТЕЙНЕРАХ

П. А. Волынкин, О. А. Кононюк

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В большинстве существующих стегосистем выбор областей встраивания строго определяется алгоритмами без учета особенностей используемого графического контейнера и размера встраиваемого сообщения, в результате чего однородные области изображения подвергаются «загрязнению», что приводит к ухудшению прозрачности восприятия.

В данной статье предлагается адаптивный подход к определению количества используемых наименьших значащих бит пикселя в зависимости от его принадлежности к однородной области или контурам изображения.

стеганография, графические файлы, НЗБ, контурное вложение.

Одним из наиболее известных стеганографических методов встраивания информации в пространственной области графических контейнеров является метод замены наименьшего значащего бита (НЗБ). Суть метода заключается в возможности замены наименьшего значащего бита пикселей изображения последовательностью бит скрываемого сообщения без заметного визуального искажения объекта [1]. Однако при увеличении емкости встраивания изменения в цвете пикселей становятся заметны в том случае, если они находились в однородных областях изображения. Данный недостаток метода может быть устранен путем увеличения полезной нагрузки контейнера за счет вложения большего объема информации в контуры изображения.

Контур определяется как рубеж резкого локального изменения яркости между соседствующими сегментами изображения. Такие научные дисциплины как компьютерное и машинное зрение используют механизмы обнаружения границ как инструмент выделения признаков объекта, поскольку контуры содержат наиболее важные визуальные характеристики. Основные применяемые на практике методы выделения границ базируются на вычислении градиента изображения и различаются типами используемых фильтров. Фильтр представляет собой квадратную матрицу, элементы которой называются коэффициентами маски. Фильтрацией (маскированием) называется процесс локальных преобразований путем перемещения скользящей маски фильтра по элементам изображения. Схема пространственной фильтрации приведена на рис. 1.

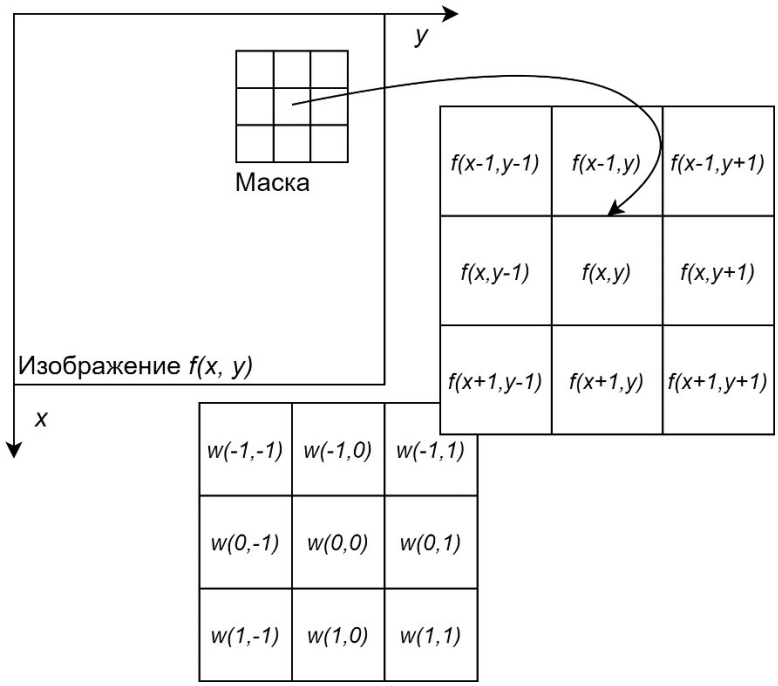


Рис. 1. Схема пространственной фильтрации

Отклик фильтрации элемента вычисляется как сумма произведений коэффициентов маски на соседние к элементу значения пикселей в соответствии с их индексами:

$$R = w(-1,-1)f(x-1,y-1) + w(-1,0)f(x-1,y) + \cdots +$$
$$+w(0,0)f(x,y) + \cdots + w(1,0)f(x+1,y) + w(1,1)f(x+1,y+1),$$

или

$$R = \sum_{i=-1}^{1}\sum_{j=-1}^{1} w(i,j)f(x-i,y-j),$$

где $w(i,j)$ – коэффициенты маски,

$f(x-i,y-j)$ – значения пикселей с относительными значениями координат.

Оператор Собеля использует маску 3×3 и выполняет свертку исходного изображения по оси x и y для вычисления приближенных значений производных [2, 3]:

$$G_x = \begin{bmatrix} +1 & 0 & -1 \\ +2 & 0 & -2 \\ +1 & 0 & -1 \end{bmatrix} * A; \quad G_y = \begin{bmatrix} +1 & +2 & +1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix} * A,$$

или

$$G_x = \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} * ([+1 \quad 0 \quad -1] * A); \quad G_y = \begin{bmatrix} +1 \\ 0 \\ -1 \end{bmatrix} * ([1 \quad 2 \quad 1] * A),$$

где A – исходное изображение.

Маски на входном изображении используются индивидуально для получения отдельных измерений G_x и G_y в направлениях x и y соответственно. В случае, если некоторые соседние элементы отсутствуют их значения принимают равными величине соседних к недостающим элементам пикселей. Путем использования приближенных значений производных для каждого элемента изображения вычисляется абсолютная величина градиента:

$$G = \sqrt{G_x^2 + G_y^2},$$

а также направление градиента:

$$\theta = -\tan^{-1}(G_y/G_x).$$

Использование оператора Прюитта аналогично оператору Собеля за исключением применения коэффициента равного единице для средних элементов маски [4, 5]:

$$G_x = \begin{bmatrix} +1 & 0 & -1 \\ +1 & 0 & -1 \\ +1 & 0 & -1 \end{bmatrix} * A; \quad G_y = \begin{bmatrix} +1 & +1 & +1 \\ 0 & 0 & 0 \\ -1 & -1 & -1 \end{bmatrix} * A.$$

Операторы Собеля и Прюитта можно успешно использовать для автоматических сегментации и определения контуров в изображении для последующего вложения информации, поскольку для любого изображения воспроизводится единственный результат такого определения.

Схема стегосистемы с определением контуров представлена на рис. 2.

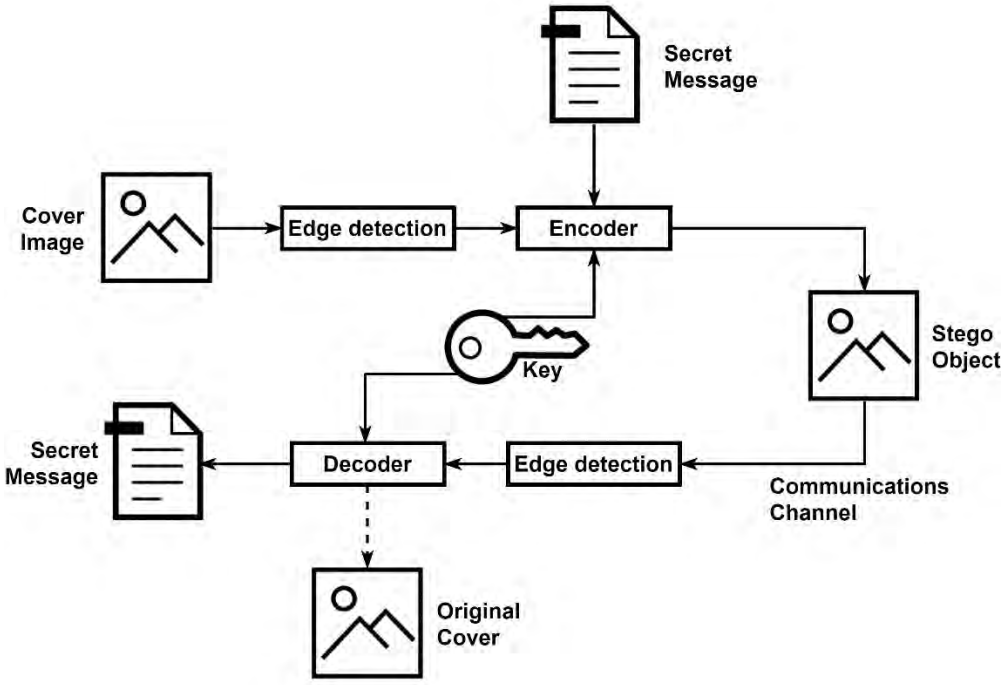


Рис. 2. Схема стегосистемы с определением контуров

При проектировании стегосистемы необходимо учитывать возможное изменение контуров после осуществления вложения. Для вложения рекомендуется использовать контуры, выявленные с наибольшим приближенным значением величины градиента, т. к. данные контуры обладают максимальной степенью устойчивости.

Помимо идентификации контуров изображения, однородные области также могут быть использованы для сокрытия информации, что обеспечивает эффективное использование контейнера, посредством увеличения его полезной ёмкости. На основе полученного контура операторами Собеля, Прюитта, Робертса или Кэнни, пиксели исходного изображения классифицируются на две категории: принадлежащие однородной области или контуру контейнера. Количество используемых НЗБ определяется параметрами k_e для контуров и k_s для однородных сегментов, где $k_e > k_s$.

Предложенный адаптивный метод НЗБ обладает большей надежностью, по сравнению с классическим методом НЗБ, а также высокой полезной нагрузкой при наименьшем искажении контейнера. Дальнейшие модификации описанного подхода подразумевают использование стегоключей для определения последовательности встраивания информации в определяемые методом области растровых графических контейнеров.

Список используемых источников

1. Коржик В. И., Небаева К. А., Герлинг Е. Ю., Догиль П. С., Федянин И. А. Цифровая стеганография и цифровые водяные знаки. Часть 1. Цифровая стеганография / Под общ. ред. проф. В. И. Коржика. СПб.: СПбГУТ, 2016. 226 с. ISBN 978-5-89160-125-3.
2. Sobel, I. An Isotropic 3x3 Image Gradient Operator. 2014.
3. Sushanta, K. M.; Shailendra, T. Edge Detection using Sobel Technique // Journal of Critical Reviews. Vol. 7. 2020. Pp. 929–933.
4. Prewitt, J. M. S. Object enhancement and extraction. Picture Processing and Psychopictorics, Academic Press. 1970.
5. Dim, Jules R., Takamura, Tamio. Alternative Approach for Satellite Cloud Classification: Edge Gradient Application. Advances in Meteorology. 2013. Pp. 1–8.

УДК 004.58
ГРНТИ 20.51.23

ОЦЕНКА ЭСТЕТИЧНОСТИ ЦВЕТОВОЙ СХЕМЫ ГРАФИЧЕСКИХ ПОЛЬЗОВАТЕЛЬСКИХ ИНТЕРФЕЙСОВ

А. В. Вострых

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается проблема оценки эстетичности цветовой схемы графических пользовательских интерфейсов. С помощью существующих констант, полученных опытным путём в дисциплинах эргономики и инженерной психологии, планируется разработать подход способный проводить оценку интерфейсов на сложность восприятия пользователями информационно-функциональных элементов и цветовой схемы интерфейсов.

пользовательский интерфейс, параметры оценки интерфейсов, эффект стереохроматизма, цветовые ассоциации, цветовая схема.

Мир современного человека насыщен различными техническими устройствами и технологиями число которых постоянно растёт, внедряясь во все направления человеческой жизни. Многочисленные информационные системы, используемые нами сегодня, уже давно стали привычными элементами

окружающей среды и культуры. Такая тесная взаимосвязь должна характеризоваться высокой степенью удобства и удовлетворения информационных потребностей пользователей [1]. Данную задачу призваны выполнять графические пользовательские интерфейсы (далее – ГПИ), которые являются посредником между внутренней ментальной моделью пользователей и моделью реализации информационных систем. Знание физических и психологических свойств человека, его недостатков и преимуществ, позволяет грамотно спроектировать ГПИ, сделав его эффективным, надёжным и удобным [2].

Сегодня на рынке программных продуктов интерфейсы низкого качества встречаются повсеместно [3]. Это связано со многими причинами, одной из которых является отсутствие многокритериальной формализованной методики оценки интерфейсов. Многокритериальность заключается как в сложности современных программных продуктов, так и в многогранности физиологической и психологической природы человека, который получает информацию о окружающем мире посредствам различных каналов восприятия [4]. Из проведённых многочисленных исследований человека следует, что большую часть информации о внешнем мире он получает через визуальный канал восприятия [4]. Таким образом в многокритериальную методику обязана входить оценка визуальной составляющей интерфейса.

Предлагаемый подход к оценке эстетичности цветовой схемы графических пользовательских интерфейсов предлагается развивать в двух направлениях:

– оценка сложности визуального восприятия интерфейсов;

– оценка гармоничности цветовой схемы интерфейсов.

Оценка сложности визуального восприятия интерфейсов основана на многочисленных исследованиях, проведённых в таких дисциплинах, как инженерная психология, эргономика, проектирование взаимодействия, гештальт психологии, информационная архитектура, прикладная математика [3]. В таблице 1 представлены уровни оценки сложности визуального восприятия интерфейсов и входящие в их состав алгоритмы.

ТАБЛИЦА 1. Оценка сложности визуального восприятия интерфейсов

Уровни оценки	Внутренние алгоритмы
Построение множества областей по границам изменения яркости, контрастности и преобладающего тона	1. Выбор цветовой модели 2. Определение общей яркости 3. Определение контрастности изображения 4. Определение преобладающего тона 5. Выделение контуров изображения с помощью алгоритма Превитта 6. Идентификация контуров метод «Наращивания областей»
Минимизация количества полученных областей в соответствии с заданными критериями	7. Сравнение результатов с принципами гештальтпсихологии

Уровни оценки	Внутренние алгоритмы
Выделение подмножеств низкой и высокой контрастности	8. Применение алгоритма FOREL
Анализ полученных подмножеств на загруженность точками концентрации внимания	9. Применение методов компьютерного зрения
10. Анализ полученных результатов и сопоставление их с моделью пользователей	

Итогом работы подхода станут как числовые оценки, определённой бальной шкалы, так и характеристические карты, представляющие результаты вычислений в виде оценочной матрицы. С помощью подхода возможно будет оценить такие параметры ГПИ, как структурность, читабельность, понятность, эффективность.

Оценка гармоничности цветовой схемы интерфейсов позволяет оценить такие параметры, как привлекательность, понятность, субъективная удовлетворённость. В таблице 2 представлены уровни оценки гармоничности цветовой схемы и входящие в их состав алгоритмы.

ТАБЛИЦА 2. Оценка гармоничности цветовой схемы интерфейсов

Последовательность оценки	Внутренний алгоритм
Определение числа цветов, использованной палитры	1. Применение метода *k*-средних
Оценка эффективности цветовой схемы	2. Сравнение с эталоном (не более 4–5 различных цветов)
Анализ гармоничности цветовой схемы	3. Сравнение с моделью пользователей (Цветовая схема – гендер)
Анализ ассоциативного восприятия цвета	4. Кластеризация по критерию соответствия цвета элемента интерфейса к его функциональному назначению;
5. Анализ полученных результатов и сопоставление их с моделью пользователей	

Итогом работы подхода станут как числовые оценки, определённой бальной шкалы, так и характеристические карты, представляющие результаты вычислений в виде оценочной матрицы.

Полученные результаты обоих подходов обобщаются и сопоставляются с моделью пользователей целевой аудитории. Параметры модели пользователей подбираются в соответствии с различными статистическими данными и константами, полученными в ходе исследований. Примерами статистических данных могут быть предпочтения по выбору доминирующих цветов в соответствии с гендером, или устоявшиеся за долгое время связи цвет – ассоциация с функциональностью, таблица 3.

ТАБЛИЦА 3. Влияние гендера на предпочитаемые цветовые схемы

Цвет	Предпочтение мужского пола		Предпочтение женского пола		Возможность использования в ГПИ	Ассоциации с функциональностью
	+%	-%	+%	-%		
Красный	7%	2%	9%	1%	0,13	Опасность, ошибка
Оранжевый	5%	22%	4%	33%	-0,46	Призыв к действию
Желтый	1%	13%	3%	13%	-0,22	Предупреждение
Зелёный	13%	3%	14%	4%	0,2	Безопасность
Синий	50%	1%	35%	1%	0,83	Обязательные условия
Фиолетовый	1%	22%	23%	5%	-0,03	Нейтральное событие
Чёрный	15%	1%	6%	1%	0,19	Нейтральное событие
Коричневый	2%	27%	3%	20%	-0,42	Нейтральное событие
Серый	3%	4%	1%	17%	-0,17	Нейтральное событие
Белый	2%	4%	1%	3%	-0,04	Нейтральное событие

Примерами констант являются: абсолютная чувствительность зрения, диапазон воспринимаемых яркостей, «эффект Пуркинье», чувствительность глаза к различению цветового тона, «эффект стереохроматизма», область ясного виденья, предельное количество цветов, используемых в ГПИ и т. д. [5]. Данный перечень констант и статистических данных, в настоящее время обобщается и систематизируется автором настоящей статьи для дальнейшего внедрения в разрабатываемый программный продукт для проведения автоматизированной оценки [6].

Таким образом, разработанный подход к оценке эстетичности цветовой схемы ГПИ, позволяет проводить оценку ГПИ и сравнивать интерфейсы между собой по таким параметрам, как структурность, читабельность, понятность, привлекательность и субъективная удовлетворённость.

Список используемых источников

1. Вострых А. В. Сравнительный анализ методов оценки человеко-машинных интерфейсов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2019). IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 2. С. 179–184.

2. Уэйншенк С. 100 главных принципов дизайна. СПб.: Питер, 2012. 272 с.

3. Сергеев С. Ф. Введение в инженерную психологию и эргономику иммерсивных сред: Учебное пособие. СПб.: Изд-во СПбГУ ИТМО, 2011. 258 с.

4. Ахунова Д. Г., Вострых А. В. Преимущества перехода на целеоринтированное проектирование интерфейсов для мобильных пользователей информационных систем // «РОСИНФОКОМ-2019». СПб., 2019. С. 5–9.

5. Демидов В. Как мы видим то, что видим. М.: Знание, 1987. 208 с.

6. Вострых А. В., Шидловский Г. Л., Лимонов Б. С. Алгоритм оценки графической архитектуры специализированных ПС используемых в подразделениях МЧС России // Научно-

аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2020. № 3. С. 127–136.

Статья представлена научным руководителем, доктором технических наук, профессором М. В. Буйневичем.

УДК 004.056
ГРНТИ 81.93.29

МОДЕЛЬ ПРОЦЕССА УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ БАЗ ДАННЫХ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

А. В. Горохов, В. С. Косолапов, В. А. Липатников

Военная академия связи

В современных условиях любая деятельность сопряжена с оперированием большими объемами информации, которое производится широким кругом лиц. Цель: Разработка модели процесса управления безопасностью баз данных в информационно-вычислительной сети. Защита данных от несанкционированного доступа является одной из приоритетных задач при проектировании любой информационной системы. Следствием возросшего в последнее время значения информации стали высокие требования к конфиденциальности данных. Результаты: определение значений характеристик нарушения безопасности, важных для принятия решения по реагированию на выявленный компьютерный инцидент, осуществляется с использованием когнитивной карты. Системы управления базами данных, в особенности реляционные СУБД, стали доминирующим инструментом в этой области. Новизна заключается в определении значений характеристик информационной безопасности базы данных. Практическая значимость: разработанная модель позволила определить дальнейшие сценарии развития информационной безопасности базы данных. Обеспечение информационной безопасности СУБД приобретает решающее значение при выборе конкретного средства обеспечения необходимого уровня безопасности организации в целом.

информационная безопасность, информационная безопасность систем управления баз данных, процесс управления безопасностью баз данных, модель когнитивной карты.

Введение

Системы управления базами данных стали основным инструментом, обеспечивающим хранение больших массивов информации. В настоящее время пристальное внимание уделяется проблемам обеспечения информационной безопасности (ИБ), которая определяет степень безопасности организации, учреждения в целом [1].

Атаки на хранилища и БД информационно-вычислительной сети (ИВС) являются одними из самых опасных для предприятий и организаций. Злоумышленников интересуют такие виды информации, как внутренняя операционная информация, персональные данные сотрудников, финансовая информация, интеллектуальная собственность, исследования рынка/анализ деятельности конкурентов, платежная информация. Эти сведения в итоге хранятся в корпоративных хранилищах и БД различного объема [2]. Для базы данных обычно требуется комплексное программное обеспечение, которое называется системой управления базами данных (СУБД). СУБД упрощает контроль и управление базами данных, позволяя выполнять различные административные операции, такие как мониторинг производительности, настройка, а также резервное копирование и восстановление.

Поскольку информация в базе данных носит конфиденциальный характер, она представляет интерес у злоумышленника. Ввиду чего возникает актуальность обеспечения информационной безопасности базы данных.

В целях защиты информации в базах данных важнейшими являются следующие аспекты ИБ:

– доступность (возможность получить некоторую требуемую информационную услугу);

– целостность (непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

– конфиденциальность (защита от несанкционированного прочтения).

Релевантные работы

В работе [3] рассматривается метод управления кибернетической безопасностью. В работе [4] рассматривается повышение эффективности обнаружения атак и принятия решений на основе оперативной оценки риска функционирования ИВС с использованием динамических моделей на основе нечетких когнитивных карт. В работе [5] рассматривается Система показателей качества баз данных автоматизированных систем. Однако, не рассмотрены вопросы ИБ системы управления базами данных, а также диагностирования инцидентов с использованием когнитивной карты [6].

На рис. 1 – представлена схема ИВС организации с сервером базы данных.

На рис. 2 – алгоритм работы системы управления базами данных ИВС.

На рис. 3 – представлен алгоритм атаки на СУБД.

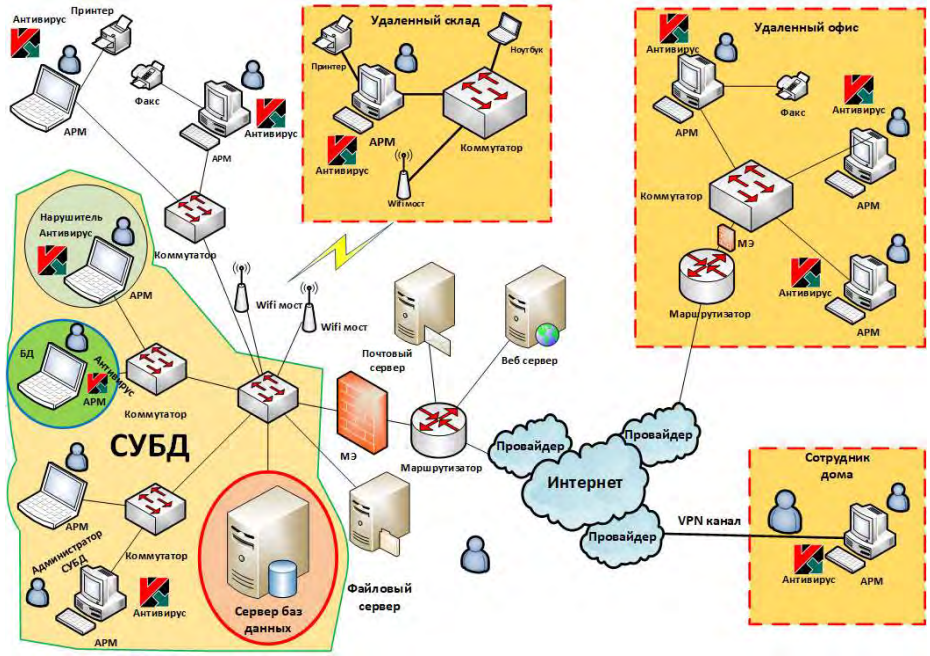


Рис. 1. Схема ИВС организации с сервером базы данных

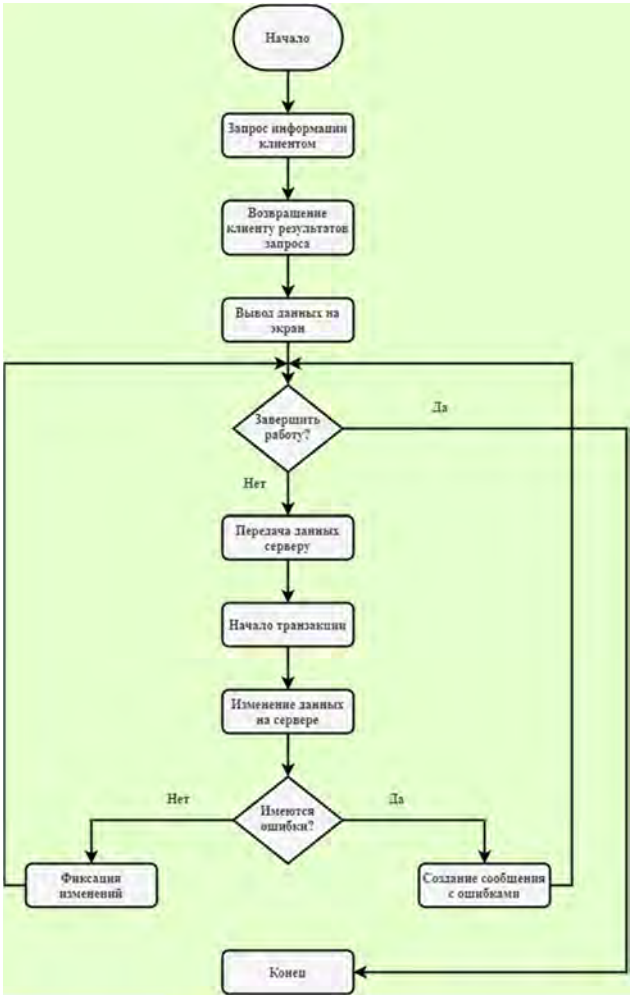


Рис. 2. Алгоритм работы системы управления базами данных ИВС

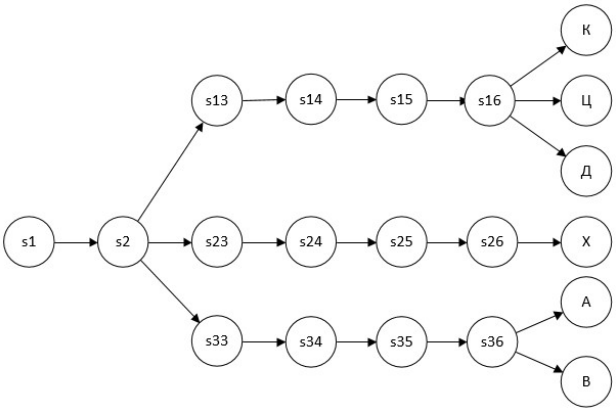


Рис. 3. Граф осуществления атак на СУБД

S1 – Начало действий нарушителя;

S2 – Сбор информации о ИВС, для реализации атаки.

Атака на конфиденциальность, целостность и доступность:

S13 – Поиск баз данных;

S14 – Анализ баз данных, выбор цели атаки;

S15 – Поиск уязвимостей СУБД;

S16 – Подбор метода воздействия на СУБД, для реализации атаки

на конфиденциальность, целостность и доступность;

К – Реализация атаки на конфиденциальность;

Ц – Реализация атаки на целостность;

Д – Реализация атаки на доступность.

Атака на пароли:

S23 – Внедрение в систему;

S24 – Построение топологии сети;

S25 – Выявление систем аутентификации и авторизации;

S26 – Подбор паролей;

Х – Реализация угрозы кражи информации.

Атака с использованием SQL инъекций:

S33 – Поиск баз данных;

S34 – Анализ баз данных, выбор цели атаки;

S35 – Поиск и подбор уязвимостей;

S36 – Внедрение SQL инъекции;

А – Реализация угрозы кражи информации;

В – Реализация угрозы кражи паролей.

Ниже представлено дерево атаки на конфиденциальность, целостность и доступность.

$$S_{КЦД} = \{S1; S2; S13; S14; S15; S16; К; Ц; Д\}.$$

Ниже представлено дерево атаки на пароли.

$$S_{ПАР} = \{S1; S2; S23; S24; S25; S26; Х\}.$$

Ниже представлено дерево атаки с использованием SQL инъекций.

$$S_{SQL} = \{S1; S2; S33; S34; S35; S36; А; В\}.$$

С ростом возможностей злоумышленника и развития информационных темпов возникают противоречия в области обеспечения информационной безопасности [7, 8]. В целях повышения ИБ базы данных предлагается рассмотреть когнитивную карту, в основу которой входит когнитивное моделирование – определение, в том числе с применением компьютера, наиболее эффективных управленческих решений и/или сценариев развития событий на основе выделения понятий (концептов, факторов), количественно и качественно характеризующих складывающуюся ситуацию, а также оценки взаимовлияния факторов. Внедрение когнитивной карты позволит определить наиболее эффективные решения и сценарии развития ИБ базы данных [9].

Заключение

Модель процесса управления безопасностью баз данных в ИВС позволяет проводить определение значений характеристик нарушения безопасности, важных для принятия решения по реагированию на выявленный компьютерный инцидент. Исследовав топологию сети военного назначения и рассмотрев графы атак на СУБД, было проведено исследование модели процесса управления безопасностью баз данных в информационно-вычислительной сети военного назначения. Новизна заключается в определении значений характеристик ИБ базы данных. Практическая значимость: разработанная модель позволила определить дальнейшие сценарии развития информационной безопасности базы данных. Целесообразно на основе когнитивной карты, проводить определение дальнейших сценариев атак и обеспечивать ИБ базы данных.

Список используемых источников

1. Основы информационной безопасности систем управления базами данных. Энциклопедия по экономике. 481 с.

2. Полтавцева М. А., Хабаров А. Р., Безопасность баз данных: проблемы и перспективы // Программные продукты и системы. 2016. № 3. С. 36–41. doi: 10.15827/0236-235X.115.036-041.

3. Липатников В. А., Тихонов В. А., Шевченко А. А. Метод управления кибернетической безопасностью в системах критических инфраструктур, основывающийся на интеллектуальных сервисах защиты информации // Технологии построения когнитивных транспортных систем. Материалы всероссийской научно-практической конференции с международным участием. СПб., 2019. С. 207–214.

4. Свечников Л. А. Интеллектуальная система обнаружения атак на основе имитационного моделирования с использованием нечетких когнитивных карт. Автореферат дисс. … канд. техн. наук: 05.13.19 / Свечников Лаврентий Александрович. Уфа, 2010. 16 с.

5. Бойко А. А., Гриценко С. А., Храмов В. Ю. Система показателей качества баз данных автоматизированных систем // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2010. № 1. С. 39–45,

6. Костарев С. В., Карганов В. В., Липатников В. А., Технологии защиты информации в условиях кибернетического противоборства: Науч. монография / Под общ. ред. В. А. Липатникова. СПб.: ВАС, 2020. 716 с.: ил. ISBN 978-5-91690-044-6

7. Липатников В. А., Шевченко А. А. Способ контроля уязвимостей при масштабировании автоматизированной системы менеджмента предприятия интегрированной структуры // Информационные системы и технологии. 2016. № 2 (94). С. 128–140.

8. Липатников В. А., Шевченко А. А., Яцкин А. Д., Семенова Е. Г. Управление информационной безопасностью организации интегрированной структуры на основе выделенного сервера с контейнерной виртуализацией // Информационно-управляющие системы. 2017. № 4 (89). С. 67–76. doi: 10.15217/issn1684-8853.2017.4.67.

9. Липатников В. А., Чепелев К. В., Шевченко А. А. Способ защиты информационно-вычислительной сети от вторжений. Патент на изобретение RU 2705773 C1, 11.11.2019. Заявка № 2019100252 от 09.01.2019.

УДК 004.3
ГРНТИ 19.51.61

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ ДЛЯ ЧТЕНИЯ ЭЛЕКТРОННЫХ ИЗДАНИЙ

А. Н. Горшенина, Т. В. Мусаева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современный человек большую часть информации получает через экран мобильного телефона, причем постоянно и из разных источников. СМИ борются в этом потоке за внимание читателей, и коммерческим печатным издательствам приходится адаптироваться к новому, электронному формату, чтобы сохранить и преумножить свою аудиторию. В работе исследуются мобильные приложения, являющиеся площадкой для размещения одного или нескольких цифровых изданий, с целью выявления общих функциональных и интерфейсных решений, их оценки и сравнения. Сравнительный анализ затрагивает паттерны подачи информации, особенности навигации, отличия материала от печатного формата и удобство использования. Результаты исследования могут быть использованы изданиями при адаптации в цифровой среде, а также стать основой новых паттернов размещения контента и взаимодействия с ним.

средства массовой информации, журнал, мобильные приложения.

В связи с нестабильной ситуацией на рынке печатных СМИ, связанной с падением интереса аудитории и ростом влияния цифровых технологий на человеческую жизнь, издательства постоянно ищут доступные и выгодные им способы перехода в медиапространство сети Интернет. Кто-то использует его только как средство распространения и продажи (интернет-магазины электронных и печатных копий), а кто-то задействует новые возможности и меняет формат подачи контента, становясь частью онлайн-библиотек или создавая собственный сервис для чтения с цифровых устройств.

Переход публикаций с бумаги в такие приложения не может быть легким. В. Е. Бирюков в статье «Визуальные и структурные признаки периодических изданий и особенности их переноса в цифровую среду» раскрывает основные понятия и отличительные особенности периодических изданий, а также предлагает некоторые решения по переносу этих особенностей в цифровой формат: колонтитул можно заменить на навигацию и поиск, обложку выпуска на простую миниатюру для идентификации, а номера журналов на бесконечную ленту статей и других материалов [1]. При этом электронные издания имеют значительные преимущества перед печатными: гипертекст, анимации, интерактивные тесты и сбор статистики [2].

Также характер изменений будет зависеть от целевой платформы, с которой будет читаться журнал. Мобильные устройства имеют ряд ограничений,

связанных с вертикальным расположением контента и небольшим количеством видимого пространства, однако основная доля потребления информации современным человеком приходится именно на них. У некоторых онлайн-ресурсов издательских домов России темп роста мобильной аудитории даже опережает средние показатели по сегменту [3], а время медиапотребления потенциально равно времени бодрствования [4].

С целью выявления интерфейсных решений, используемых цифровыми изданиями в рамках формата мобильных приложений, проанализированы ресурсы, перечисленные в таблице. Исследуемые журналы имеют печатный аналог и находятся в открытом доступе на мобильной платформе Android через сервис «Google Play». Приложения могли быть агрегаторами различных журналов, а могли полностью представлять один конкретный.

ТАБЛИЦА. Анализируемые приложения

Название	Количество скачиваний	Тип
Zinio	Более 50 млн.	Онлайн-библиотека
Pablish	Более 10 тыс.	Онлайн-библиотека
PressReader	Более 5 млн.	Онлайн-библиотека
Vogue	Более 10 тыс.	Отдельный журнал
The New York Times	Более 10 млн.	Отдельный журнал

Приложениям для отдельных журналов, в отличие от онлайн-библиотек, намного легче изменять представление контента. Множество разных по тематике, подаче и визуальному оформлению изданий без дополнительной подготовки практически невозможно объединить одним форматом без потери качества материала, поэтому распространяемые через онлайн-библиотеки номера зачастую выглядят так же, как и печатные, но снабжены рядом дополнительных функций, таких как навигация и предпросмотр. Приложения же отдельных журналов сильно меняют формат, делая его удобным для чтения с телефона. Компромисс между ними пыталось создать «Zinio», в котором PDF-файлы журнальных страниц автоматически преобразовываются в текст и сопутствующие изображения, однако такой подход существенно влияет на визуальную привлекательность и иногда понятность материала (рис. 1).

Во всех исследуемых приложениях, кроме «The New York Times», используется горизонтальная навигация через предпросмотр страниц. В случае журнала «Vogue» пользователь увидит верхние части статей, раскрывающие основную суть. Также в части приложений реализована вертикальная навигация по основным частям выпуска - интерактивное оглавление (рис. 2).

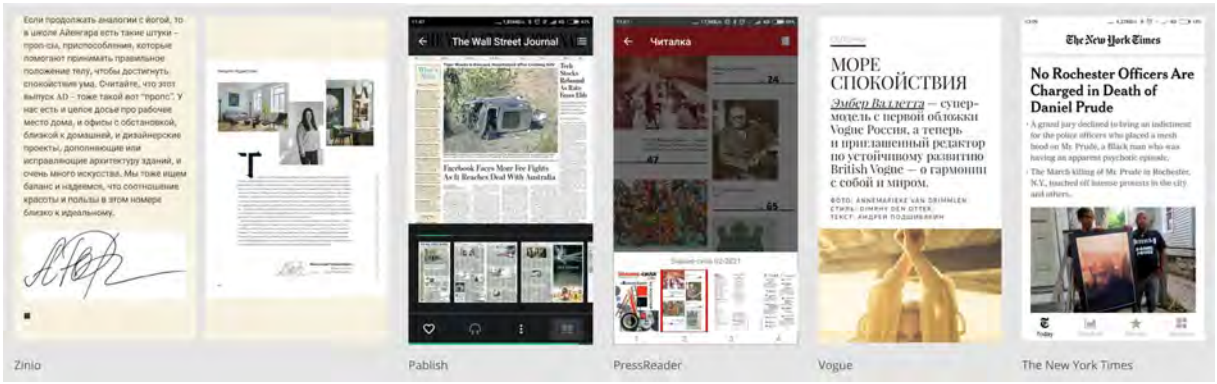


Рис. 1. Формат чтения выпусков

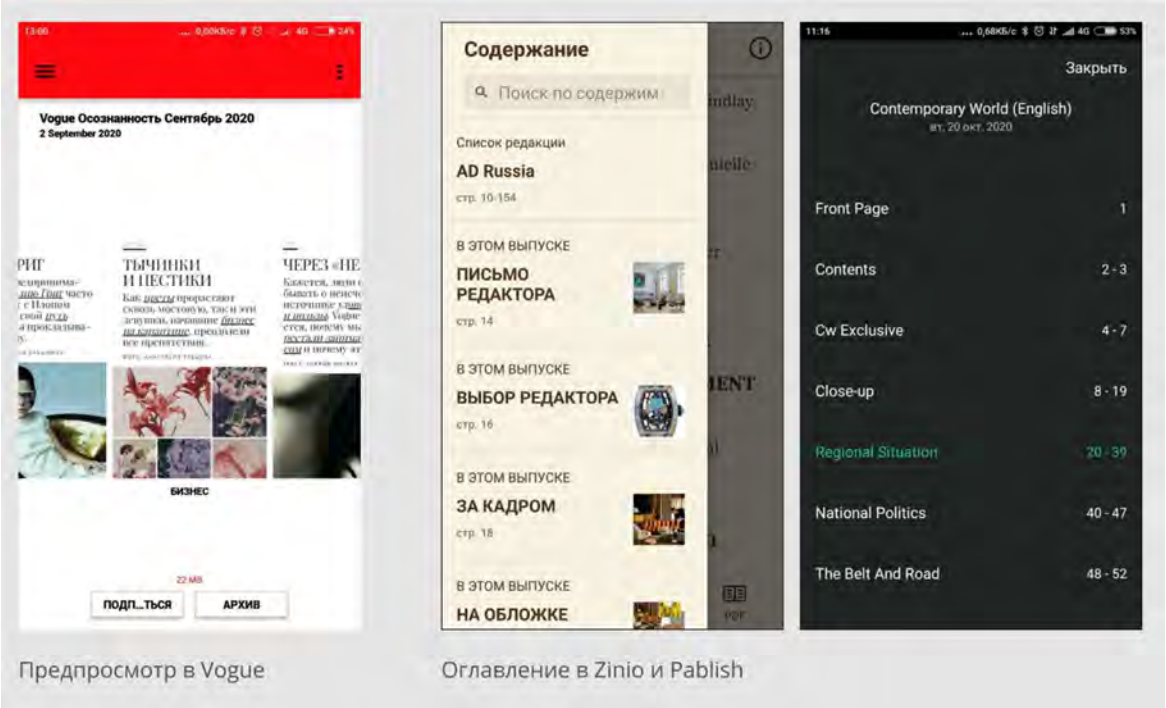


Рис. 2. Навигация

Для привлечения внимания читателей к платному контенту (подписка, покупка выпуска) почти во всех приложениях используется механизм статей. В открытом доступе находится небольшая законченная часть материала, которая показывает характер и качество содержащегося в журнале контента (рис. 3). Любая статья или ее часть должна содержать ссылку на выпуск или полный текст.

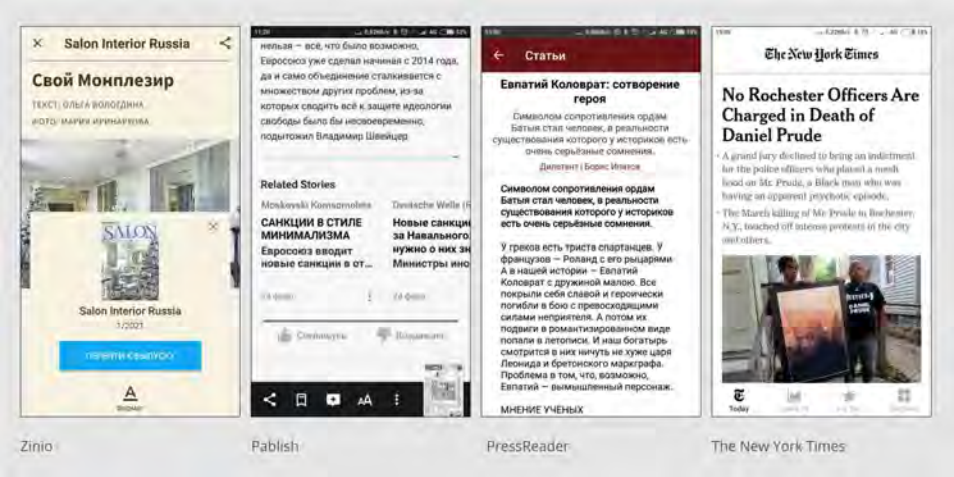


Рис. 3. Статьи

Со статьями и выпусками зачастую также связаны социальные взаимодействия: отправка обратной связи, возможность поделиться в социальных сетях (рис. 4).

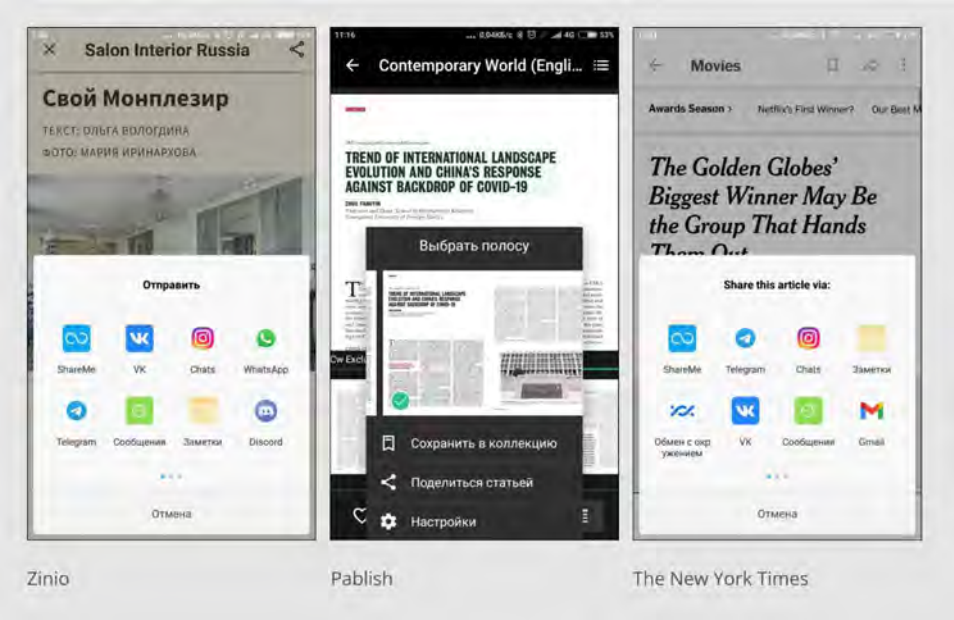


Рис. 4. Отправка статьи в социальных сетях

Не распространенными, но удобными для пользователя решениями являются настройки размеров и цветов при чтении, использование гиперссылок на внешние или внутренние ресурсы и рекомендации с подбором подобных статей.

Выявленные интерфейсные решения могут использоваться при создании платформы, которая поможет издательству наиболее безболезненно перейти на новый, цифровой формат, а затем увеличить свою аудиторию.

Список используемых источников

1. Бирюков В. Визуальные и структурные признаки периодических изданий и особенности их переноса в цифровую среду // Московская государственная художественно-промышленная академия им. С. Г. Строганова. Москва, 2013. С. 300–308.

2. Редакторская подготовка изданий: Учебник / Антонова С. Г., Васильев В. И., Жарков И. А., Коланькова О. В., Ленский Б. В., Рябинина Н. З., Соловьев В. И.; под общ. ред. Антоновой С. Г., д. ф. н. М.: Издательство МГУП, 2002. 468 с.

3. Состояние, тенденции и перспективы развития. Отраслевой доклад. 2019 / Ред. Григорьев В. Федеральное агентство по печати и массовым коммуникациям, Управление периодической печати, книгоиздания и полиграфии. Российская периодическая печать. С. 7–9.

4. Судьба печатной прессы в эпоху Интернета : коллектив. моногр. / М. В. Загидуллина, С. И. Симакова, Л. Г. Александров, Л. Г. Свитич и др.; под ред. М. В. Загидуллиной, С. И. Симаковой. Челябинск : Изд-во Челяб. гос. ун-та, 2018. 181 с.

УДК 004.7
ГРНТИ 81.93.29

АКТУАЛЬНОСТЬ МЕТОДОВ БОРЬБЫ С DDOS АТАКАМИ

Н. А. Гришин, Н. А. Косов, П. С. Мазепин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Цель исследования – проанализировать актуальность методов борьбы с DDOS атаками, которые на сегодняшний момент являются одним из популярных способов атак, направленных на вычислительную систему с цель довести ее до отказа. В статье рассмотрены наиболее популярные и в то же время эффективные методы противодействия данному типу атак. Отдельно будет рассмотрена стоимость реализации каждого из методов и области их применения. Также, будут рассмотрены основные плюсы и минусы каждого из методов и представлены пути развития определенных методов с целью увеличения их эффективности. В результате будет выбран оптимальный метод борьбы, опираясь на стоимость реализации и эффективности.

DOS, DDOS, информационная безопасность, отказ в обслуживании.

Во времена повсеместной цифровизации в жизни общества именно безопасность данных является наиболее обсуждаемой темой множества компаний гигантов. За многие современные, как программные, так и аппаратные, методы защиты от различных атак компании готовы платить большие суммы денег, чтобы в дальнейшем не потерпеть весьма серьёзные убытки.

Множество серверов или иных удаленных ресурсов, которые обеспечивают работу практически во всех сферах жизнедеятельности общества, всегда являются одной из главных целей злоумышленников, а иногда и конкурентов.

На сегодняшний день одной из наиболее распространенной атакой на такие ресурсы является DDoS атака. Актуальность методов борьбы с которой будут рассмотрены.

DoS (Denial of Service) – атака на информационную систему, с целью довести ее до отказа, ситуации когда легитимные пользователи не смогут получить доступ к услуге (сервера, данные, порталы) или доступ будет затруднен. Во время такой атаки злоумышленник не пытается получить данные с ресурса или контроль над ним, поэтому данный тип атак имеет определенные коммерческие особенности [1].

DDoS – DoS атака с использованием большого количества компьютеров. Для осуществления такого типа атаки злоумышленнику требуется контроль над большим количеством вычислительных устройств, поэтому DDoS атаке предшествует серьезная и длительная подготовка – создание и распространение вредоносных программ, с целью создания бот-сети и использования ее во время атаки [1, 2].

В период пандемии COVID-19 и сопутствующих событий, резко увеличилось количество постоянно активных пользователей, изменился период активности и сферы деятельности. Все это повлекло за собой серьезные изменения в сфере DDoS атак. Так, согласно отчету Ростелекома, количество DDoS атак в рунете за 2020 год увеличилось в среднем в 3 раза.

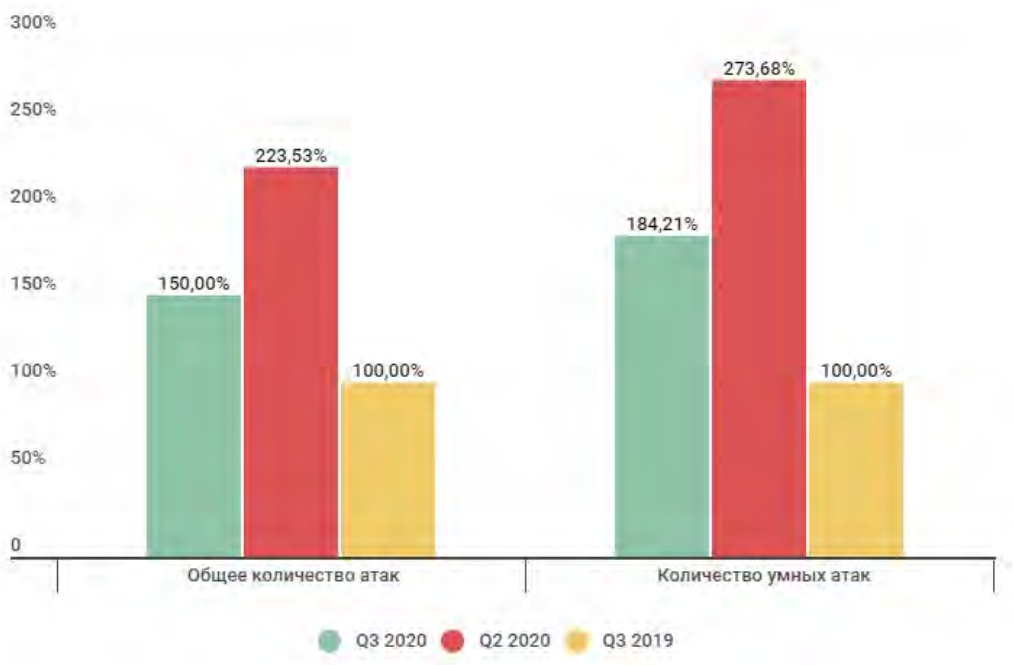


Рис. 1. Сравнительное количество DDoS-атак, Q2 и Q3 2020, а также Q3 2019. За 100 % приняты данные за Q3 2019

В то же время, изменилась и качественная характеристика атак. Если в предшествующих годах, возрастало количество сложных и мощных атак на различные бизнес-ресурсы, проводимых с целью получения финансовой выгоды, то в период пандемии резко возросло количество «любительских» (атаки простейших типов, низкой продолжительности и интенсивности) атак на образовательные, медицинские и государственные ресурсы.

DDoS атаки могут быть разных типов, но наиболее популярной с огромным отрывом, по отчетам “Kaspersky” является SYN-флуд.

Защититься от DDoS атаки достаточно сложно и иногда требует большого количества времени по нескольким причинам:

- **Врожденные уязвимости сети** – то есть использование физического ограничения по количеству запросов, которое устройство может обработать в заданное время. Для успешной атаки необходимо просто превысить данный порог. Большая часть атак может быть отражена путем обновления ПО или настройки политик, но данные методы не могут всегда обеспечить полное противодействие DDoS атакам, поскольку службы должны быть доступны всегда, а значит они всегда уязвимы для атак [3, 4].

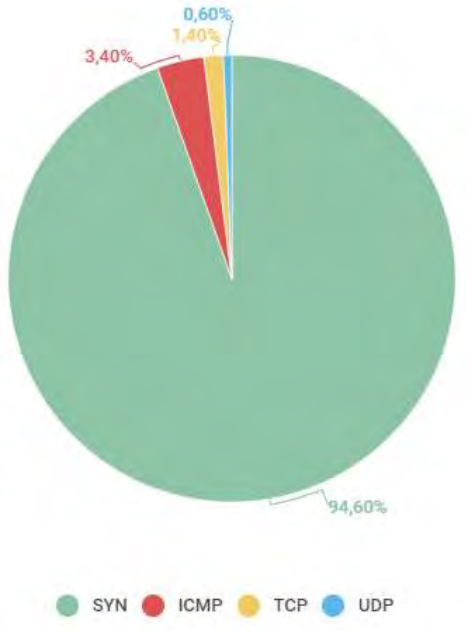


Рис. 2. Распределение DDoS-атак по типам, Q3 2020 г.

- **Невозможность заблокировать «толпу»** – по большей части DDoS атака осуществляется с очень большого пула IP-адресов и очень трудно обеспечить эффективную блокировку длинного списка этих адресов. [3, 4]
- **Фильтрация запросов** – сложно определить какие пользователи делают законные запросы, а какие участвуют в DDoS атаке. Поскольку все пользователи, получающие доступ к услугам, выполняют те или иные запросы, то по факту они все участвуют в DDoS атаке [3, 4].

На данный момент существует множество решений по борьбе с определенными типами атак, но ни один из них не может решить актуальную на данный момент проблему того, что механизм атаки может быть отличный от тех, которые данный метод блокирует и как следствие решение будет бесполезно и никак не сможет предотвратить данную атаку [3].

Существуют решения для защиты от DDoS атак как на стороне клиента, так и на уровне провайдера, а также наиболее эффективные решения, которые сочетают в себе как защиту на стороне клиента, так и на стороне провайдера [3, 4].

В данный момент существует два наиболее эффективных способов борьбы с DDoS атаками, один из которых основан на облачной аналитике больших данных, но стоимость данного решения является такой же «облачной». Но данный метод позволяет блокировать не только известные атаки, но и также противостоять новым методам осуществления атак. По данным “Qrator Labs” такие системы способны выдерживать атаки до 1 500 Гбит/с. Благодаря этому совершить атаку, которая может оказаться успешной возможно только обладая огромными вычислительными мощностями. Схожим по эффективности и стоимости реализации является использование систем распределенной защиты – соответствующее оборудование устанавливается у магистральных операторов, и если анализатор атак фиксирует нападение на защищаемый сайт или сервер, он моментально транслирует адреса атакующих хостов другим узлам по всей сети, и сеть начинает работать против атакующих хостов. Атака гасится, а то, что доходит до цели, отбивается фильтрами [3].

Таким образом, современные методы позволяют минимизировать время которое услуга является не доступна. Но проблема остается актуальной, поскольку, если есть время, которое услуга не доступна, то значит атаку можно считать успешной.

На текущий момент не существует решений, которые могут обеспечить полную защиту от DDoS атак, но системы, основанные на анализе больших данных являются достаточно перспективными и уже на текущий момент эффективными. А основной проблемой всех механизмов является их стоимость и нередко даже 4–5 дней простоя в следствии DDoS атак является наиболее экономически выгодно, чем подготовленная заранее система, которая бы смогла отразить эти атаки.

Список используемых источников

1. Бекенева Я. А. Анализ актуальных типов DDoS-атак и методов защиты от них // Известия Санкт-Петербургского государственного электротехнического университета Лэти. 2016. Т. 1. С. 7–14.

2. Савчук И. Артём Гавриченков: Борьба с DDoS-атакой–это игра краплеными картами с профессиональным шулером // Системный администратор. 2013. №. 4. С. 4–9.

3. Умутбаев Э. И., Файрузов Р. А., Кашапов Н. Р. Исследование ddos-атак и методов борьбы с ними // Международная молодежная научная конференция «XXII Туполевские чтения (школа молодых ученых)». 2015. С. 157–160.

4. Иниватов Д. П., Ануфриев Е. В., Ушабаев Р. Т. Определение списка рекомендованных действий при проведении DDOS-атак // Передовые инновационные разработки. Перспективы и опыт использования, проблемы внедрения в производство. 2019. С. 32–34.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.921
ГРНТИ 50.51.02

КОМПАС 3D-LT ВЕРСИИ 12 КАК НЕДООЦЕНЕННЫЙ ИНСТРУМЕНТ СОВРЕМЕННОЙ ИНЖЕНЕРНОЙ ГРАФИКИ

В. В. Громов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются методика обучения студентов с помощью систем автоматизированного проектирования (далее – САПР). Компас-3D версий 12–19 при выполнении учебных заданий по дисциплине «Инженерная и компьютерная графика» в Санкт-Петербургском Государственном университете телекоммуникаций им. проф. М. А. Бонч-Бруевича.

Приведенная методика основана на многолетнем опыте обучения студентов в период с 2013 по 2021 г.г. Анализируются перспективы формирования навыков создания чертежей у студентов в условиях современного развития САПР с учётом уровня подготовки современных граждан общеобразовательными и средними специальными учебными заведениями.

системы автоматизированного проектирования (САПР), программные системы, инженерная графика.

В августе 2020 г. была зарегистрирована программа для ЭВМ Система трехмерного моделирования Компас 3-D v19. С данной системой, а точнее с beta-версией этой системы я работал с 2019 года. Хотелось бы рассказать о некоторых метаморфозах, которые произошли за шесть лет знакомства с данной системой и тех методах, которые были внедрены в систему обучения по дисциплине «Инженерная и компьютерная графика» (Черчение), но для начала необходимо рассказать о тех условиях, в которых приходится работать.

В настоящее время, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича (далее – СПбГУТ), обладает лицензией для обучения студентов по дисциплине «Инженерная и компьютерная графика» с использованием Системы трехмерного моделирования Компас 3-D v16 и17.

Казалось бы, следует написать очередную докладную и расписать план развития для студентов и включить в план закупок новейшее программное обеспечение Систему трехмерного моделирования Компас 3-D v19, но поразмыслив над сложившейся ситуацией и обсудив данную ситуацию на заседании кафедры мы приняли решении повременить с обновлением системы и попробовать внедрить новые формы обучения для обучения по дисциплине «Инженерная и компьютерная графика».

Внедрение новых методик было вызвано резким снижением уровня образования студентов, а также нежеланием студентов использовать научно-техническую и методическую литературу по дисциплине.

Практические задания по дисциплине «Инженерная и компьютерная графика» включают в себя выполнение графических работ с использованием программного обеспечения «Система трехмерного моделирования Компас 3-D» по темам:

1. Чертеж детали.
2. Сборочная единица.
3. Схемы.

Студенты выполняют чертежи и схемы по указанным темам в общем объеме 13–15 листов формата А4–А2.

Для выполнения данных работ требуется компьютер и «Система трехмерного моделирования Компас 3-D». Наличие компьютера и последней версии программного обеспечения не гарантируют успешное выполнение лабораторных работ, а как следствие – получение зачета по дисциплине «Инженерная и компьютерная графика».

В СПбГУТ учатся студенты различных регионов Российской Федерации, студенты из ближнего зарубежья (Туркмения, Украина, Белоруссия), а также студенты из Африканских стран и Азиатско-Тихоокеанского региона. В течении 8 лет мы проводили анонимные опросы студентов по источникам информации для получения четкой картины природы «научного нигилизма» у студентов.

Исходя из нигилистической позиции отрицания знаний предыдущих поколений студентов можно поделить на несколько социальных групп:

1. Читающих художественную или учебную литературу (не более 10–20 %).
2. Использующих смартфоны для получения информации (около 80 %).
3. Читающих восточную литературу или комиксы (1–5 %).
4. Не читающих литературу (художественную или техническую) (5–10 %).

Естественно, данное разделение студентов – условно, но оно отражает современные реалии подготовки школьников к образовательному процессу в высших учебных заведениях (далее – вуз). Было замечено, что студенты неохотно используют учебную литературу для изучения дисциплины «Инженерная и компьютерная графика», «Физика», «Высшая математика» и др. Большинство студентов стараются использовать интернет ресурсы, но не обращают внимание на содержание данного ресурса, а как следствие на актуальность информации в целом.

Изложенные выше факты являются основной проблемой профессорско-преподавательского состава любого вуза, а как следствие на качество подготовки кадров для промышленности Российской Федерации.

Второй, более глобальной проблемой для ВУЗов является финансирование за счет студентов, привлекаемых по платным программам. Данные студенты считают, что они имеют веские основания для «особого отношения» к себе и учебе и как следствие - получение преференций на зачетах и экзаменах в отличии от студентов, проходящих обучение на факультете финансируемого из государственного бюджета. В следствии чего, за последние 4 года резко увеличилось число студентов, которые «закрывают свои долги» перед защитой диплома т.к. на это влияют факторы, которые ограничивают возможности администрации ВУЗов по порядку отчисления студентов в виду необходимости финансирования за счет привлечения студентов по «коммерческим программам» (программам платного обучения).

Учитывая, что студента можно отчислить только если он:

– не сдал 3 предмета в сессии;

– не сдал экзамен на положительную отметку после 3 раз (1 основной экзамен + 2 пересдачи);

– при переходе на другой факультет не сдал недостающие предметы;

– не сдал одну из аттестационных работ (отчеты, курсовые, ВКР, диплом специалиста).

То методов воздействия на сознательность студентов не остается, а следствием данной ситуации является, когда деканаты вынуждены использовать административный ресурс для сохранения численности студентов на факультете [1].

Я упомянул только о последствиях, которые возникают у большинства ВУЗов, но не раскрыл причин к возврату «устаревшей» «Системе трехмерного моделирования Компас 3-D» версии 12 LT. Для чего мы сделали частичный «откат» на более раннюю версию «Компас-3D» версии 12LT рассказывается в этой статье.

Обозначенные проблемы нас плавно подвели к использованию «Компас-3D» версии 12LT по следующим фактам:

1. Для работы в «Компас-3D» версии 12LT не требуется мощных вычислительных систем (достаточно планшета с 1-2ГБ ОЗУ, 32 ГБ ПЗУ с процессором Intel Baytrial-T Z3735F 1,33 ГГц и операционной системы Windows 8 или 10).

2. Отсутствие функций доступных в более старших версиях способствует развитию пространственного мышления у студентов и принятия нестандартных решений для выполнения поставленной задачи (например: создание отверстия с резьбой).

3. Изучение классических способов применения технологических приемов для реализации сложных геометрических форм.

4. Создание «искусственных барьеров» для реализации.

На рис. 1 показан пример построения детали, имеющей сложную геометрическую форму, которые многие студенты не смогли сделать за 40 минут

в «Компас-3D» версии 17-19. Данная деталь была сделана в «Компас-3D» версии 12LT специально, для того что бы доказать, что излишние ресурсы – мощный компьютер и новая среда разработки, не гарантируют быстрое выполнение задания.

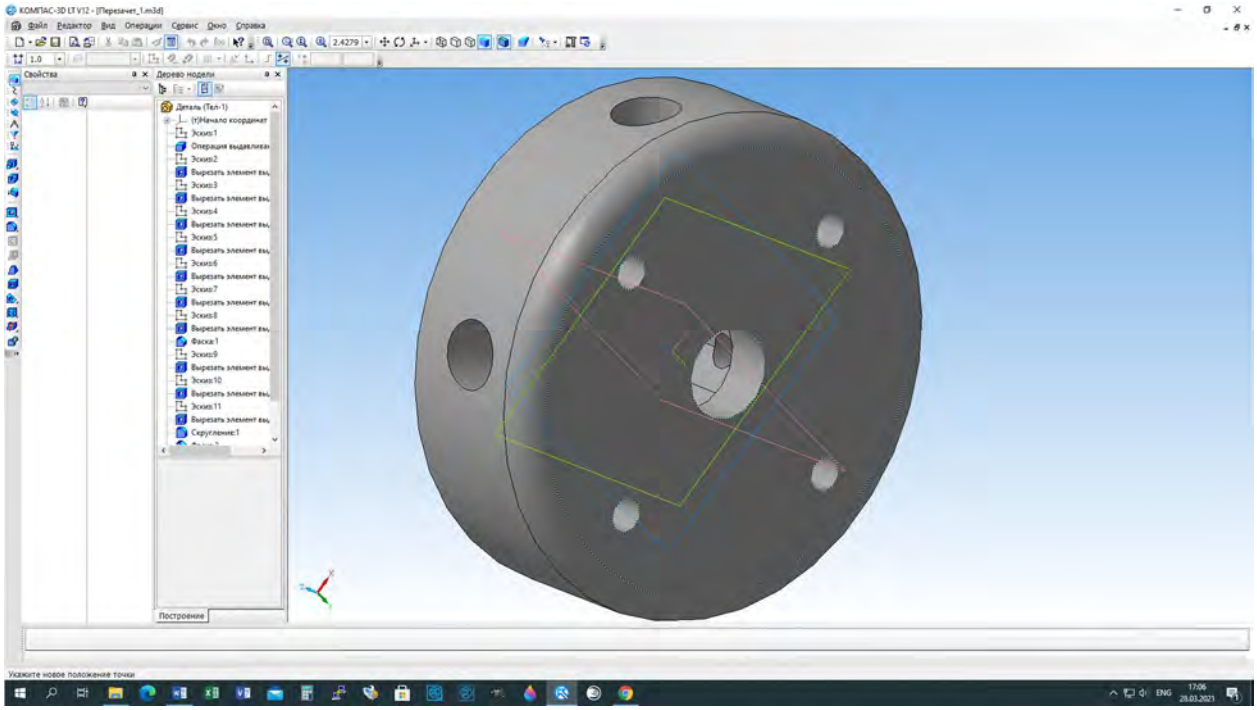


Рис. 1. Пример построения детали, имеющей сложную геометрическую форму

Сложность данного задания заключалась в том, что по торцу детали (прижимной шайбы, далее – Шайбы) расположены четыре отверстия. «Компас-3D» любой версии не дает возможность работать с круглой поверхностью, а тем более создавать на ней какие-либо объекты. Создать отверстие возможно только через функцию «Смещенная плоскость».

Существует более простой технологический способ, который позволяет создать подобный объект или деталь без «Совмещенной плоскости». Для этого надо знать технологию изготовления подобных деталей или хорошо знать курс начертательной геометрии вспомнив, что в основу любого правильного многоугольника можно вписать или описать вокруг него окружность.

В данной задаче мы можем и должны прибегнуть к основным методам начертательной геометрии и создать подобный объект без использования «Совмещенной плоскости» рис. 2 и рис. 3.

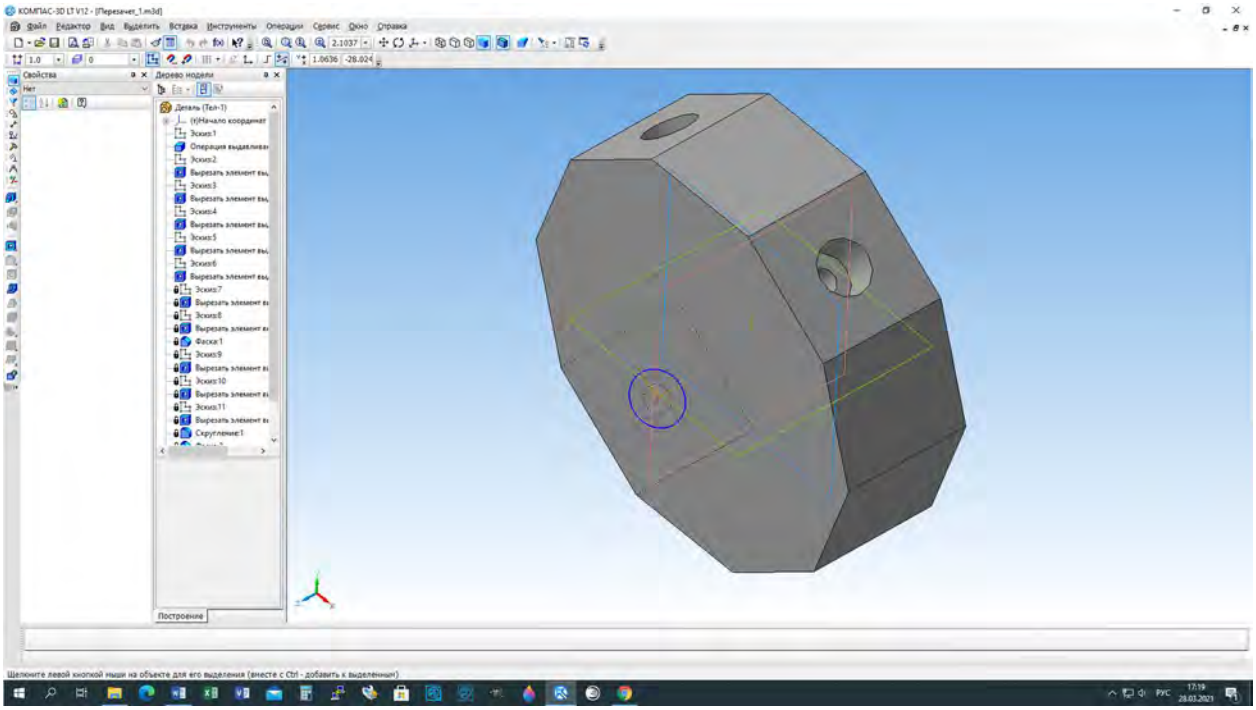


Рис. 2. Создание объекта без использования «Совмещенной плоскости»

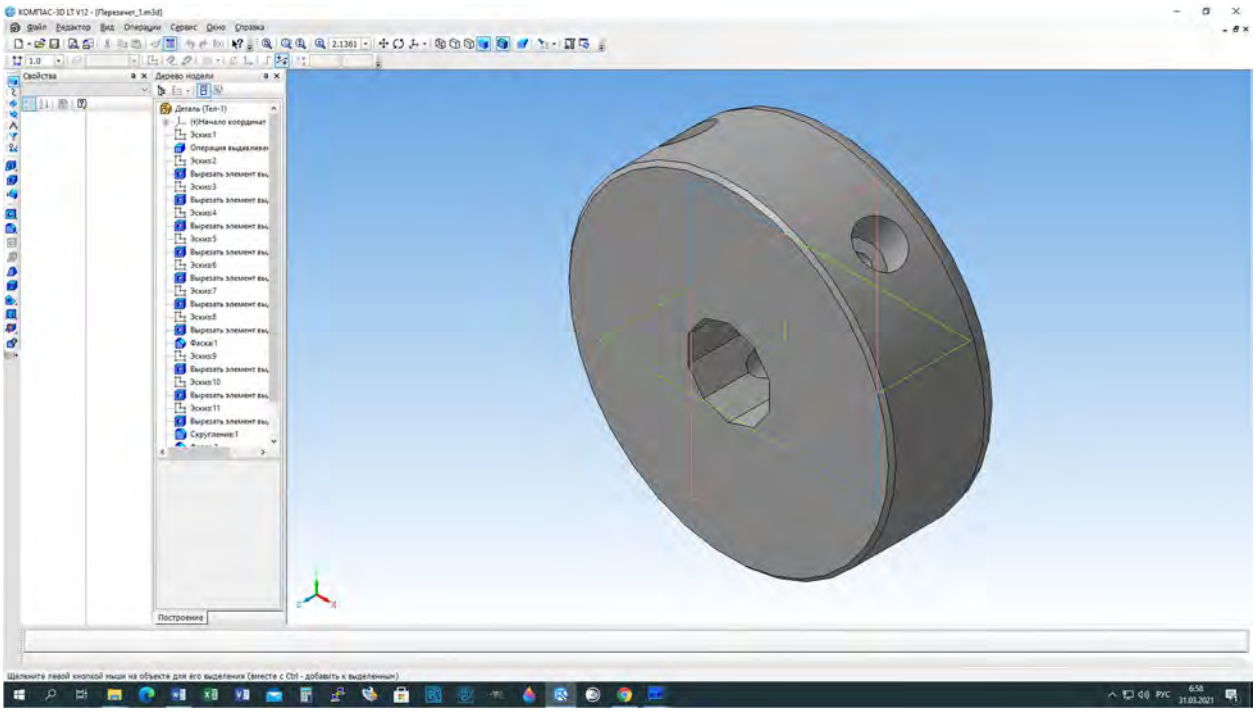


Рис. 3. Подсказка – отверстие в форме шайбы,
выполненное в форме правильного десятиугольника

Примененная методика показала, что студенты, которые читают методические указания или техническую литературу, достаточно быстро находят способ применить «Совмещенные плоскости» для построения отверстий на торце

шайбы, но ни один студент не обратил внимание на подсказку, которая достаточно хорошо видна на рис. 3 – отверстие в центре шайбы выполненное в форме правильного десятиугольника.

Многие пытались создать данное отверстие вручную откладывая отрезки по заданным угловым величинам и заданной длине, тем самым резко сократили своё время на выполнение задания. В заключении мы подошли к достаточно интересному и нужному вопросу для инженерной графики – необходимостью изучения некоторых важных аспектов курса начертательной геометрии для применения методов построения фигур и плоскостей в рамках курса Инженерная и компьютерная графика (черчение).

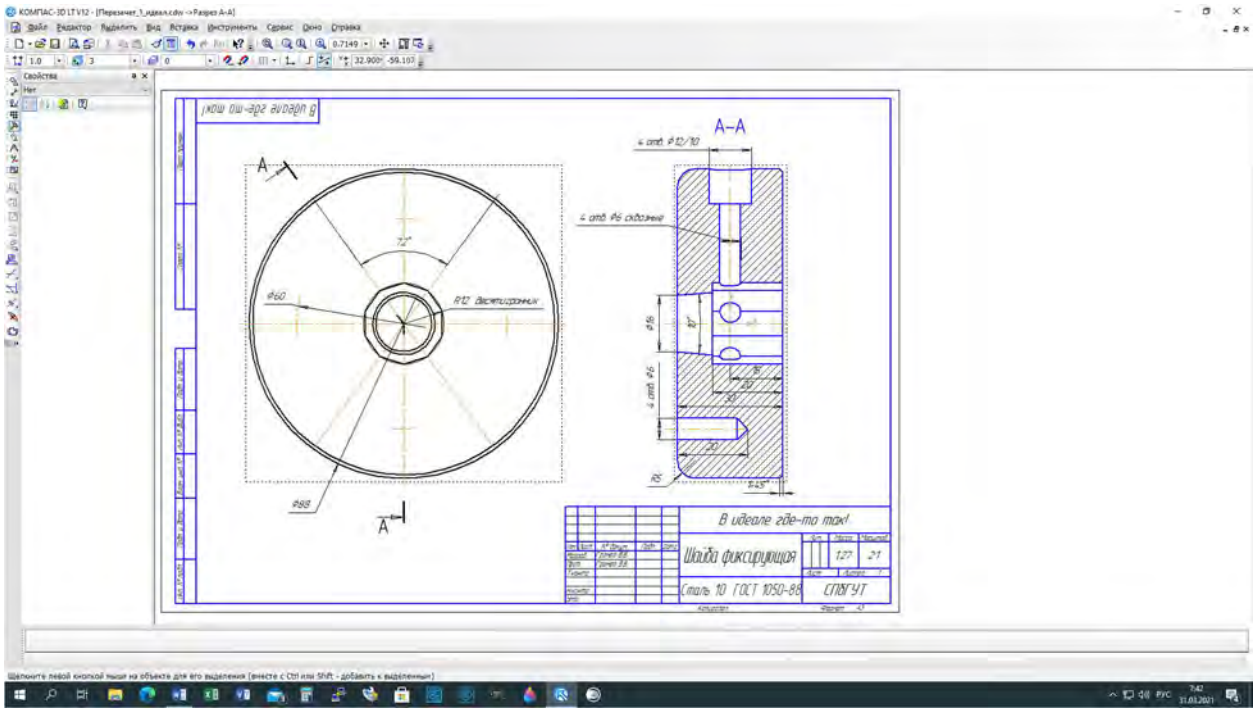


Рис. 4. Пример зачета по дисциплине

Вышеизложенные факты позволяют сделать заключение, что система образования претерпела резкие изменения, которые необходимо учитывать и восполнять при проведении практических занятий по дисциплине «Черчение» или «Инженерная и компьютерная графика» [3].

Так же было доказано, что «Компас-3D» версии 12LT способен формировать любые объекты в рамках курса «Инженерная и компьютерная графика» (черчение), за исключением модели сборочной единицы и соответственно – сборочного чертежа посредством функции проецирования модели в чертеж.

Заставляя студентов применять устаревшее программное обеспечение в заданиях начального уровня, мы формируем навыки аналитического мышления, мотивируя студента на чтение нормативной документации и методических указаний.

В заключении необходимо отметить, что без введения в школьную программу таких дисциплин как «Черчение» и «Труд» преподавание дисциплины «Инженерная и компьютерная графика» в объёме 72 часа не позволяет сформировать инженерные навыки в полном объеме у всех студентов, а как следствие требуется увеличение общего объёма до 108 или 180 часов для включения в дисциплину части материалов из курса «Начертательная геометрия».

Список используемых источников

1. Громов В. В. Основные проблемы стандартизации в России // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. С. 246–250.

2. Приказ от 27 мая 2016 г. № 1730 «Об утверждении порядка свободного доступа к документам, разрабатываемым и применяемым в национальной системе стандартизации». URL: http://www.gostinfo.ru/pages/Normrule/directacts/ (дата обращения 29.03.2020).

3. Громов В. В. Основные проблемы стандартизации в России // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. С. 198–203.

УДК 004.27
ГРНТИ 20.23.21

ПЕРСПЕКТИВЫ РАЗВИТИЯ КОМПЬЮТЕРОВ НА БАЗЕ ARM ПРОЦЕССОРОВ

В. В. Громов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются основные направления развития микрокомпьютерных систем в учебном процессе. Рассматриваются примеры создания информационных систем в учебном процессе на базе процессоров ARM. Рассматривается вопрос обучения навыкам администрирования сложных информационных систем на примере использования платформ на базе ARM-процессора.

Обсуждается возможность применения в учебном процессе современных академических программ по использованию современных операционных систем с возможностью построения макетов, имитирующих сложные промышленные системы.

микрокомпьютеры, информационные системы, процессоры ARM.

Как уже неоднократно писалось в моих статьях знакомство с микрокомпьютерами началось в с Raspberry PI первой модели, который был оснащен процессором Broadcom BCM2835, 700MHz single core ARM1176JZF-S CPU, и имел 1 024 MB оперативной памяти, работающий на чистоте 400 МГц [1].

В настоящее время для проведения экспериментальных работ был приобретен микрокомпьютер Raspberry PI 4 BCM2711 на базе ядра Cortex-A72 (ARM v8) 2 048 MB оперативной памяти, работающий на чистоте 1 500 МГц. Данный микрокомпьютер использовался мною в цикле лекций по программе «Информатика» для ознакомления студентов с возможностью изучения операционной системы Linux и применения данных компьютеров в режиме промышленной эксплуатации на базе отдела или отделения рис. 1.

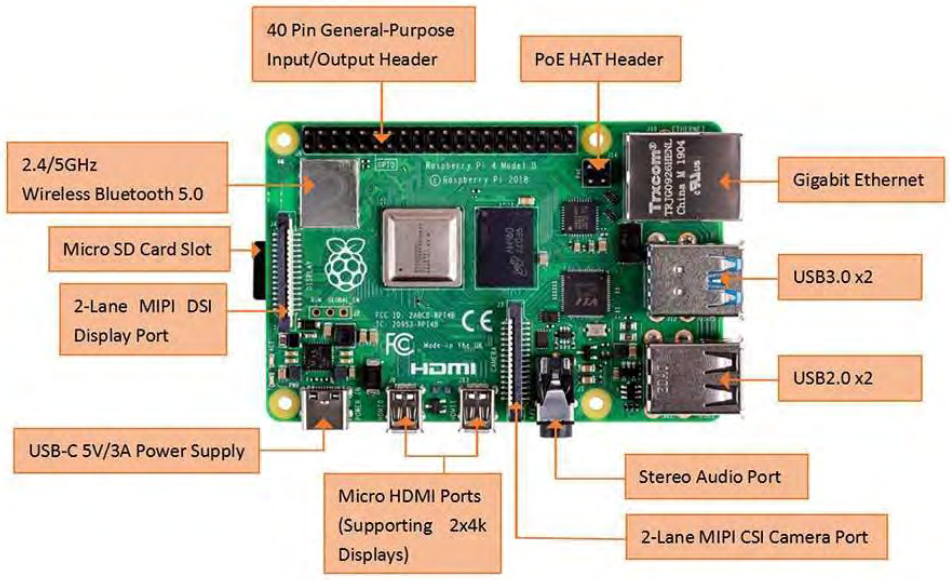


Рис. 1. Изменение модели микрокомпьютера за период с 2019 по 2020 года выпуска

На рис. 1 видно, как изменилась модель микрокомпьютера за период с 2019 по 2020 года выпуска. Не многие организации используют микрокомпьютеры в своей повседневной работе. может значительно снизить затраты на электропитание информационных систем, а также улучшить процесс обучения современных студентов. Следует отметить, что данные микрокомпьютеры были созданы для обучения школьников и студентов программированию с базовым языком Phyton, C, Assembler.

Изначально, Raspberry PI, был создан для обучения таким языкам программирования как Phyton, C, Assembler. Основной задачей при создании данного микрокомпьютера была минимальная стоимость изделия, которая должна была быть в пределах от 25$ до 35$. К чести Raspberry Pi Foundation, они справились с данной задачей, а последующее развитие технологий позволило значительно улучшить свойства и возможности данного микрокомпьютера [2].

Указанные компьютеры позволяют работать в (усеченной), специально модернизированной корпорацией Microsoft операционной системе Windows 10, а также в операционных системах семейства Linux. Применение операционной системы Linux на данном типе микрокомпьютеров позволяет значительно расширить возможности использования данного типа компьютеров в учебном процессе.

Формально, возможно создать модель промышленного сервера на базе ОС Linux использующего такие сервисы как:

1. Сетевае службы (сервисы) – SAMBA, NFS, SMTP/POP3/IMAP, TCP/IP, WWW.

2. Языки программирования – любые языки программирования, которые поддерживает операционная система, установленная на Raspberry Pi, такие как: C/C++, Pascal, Phyton, Assembler, Basic, Fortran, REXX и др.

3. СУБД использующие язык SQL и noSQL др.

4. Создание кластерных систем.

Микрокомпьютеры позволяют значительно сократить расходы на оборудование и эксплуатацию обучающих систем за счет того, что Raspberry Pi позволяет работать стандартным дистрибутивам с использованием любых стандартных наборов программ для открытых систем. На Raspberry Pi версии 3 и 4 мною были созданы серверы баз данных под управлением СУБД PostgreSQL, MariaDB, MySQL и WEB – серверы Apache и NGINX, а также CMS система Joomla для представления данных по средствам WWW серверов. Упомянутые сервера уступают серверам и рабочим станциям, оснащенным процессорами Intel Athom, Celeron, Xeon или AMD, но позволяют создать полноценный сервер для beta-тестирования.

Мне приятно было читать статьи на сайте top500.org который опубликовал последние данные на июнь и ноябрь 2020 года о производстве суперкомпьютеров. В июле 2020 года было опубликована информация о суперкомпьютере Fugaku который до настоящего времени остается лидером среди суперкомпьютеров, при этом данный суперкомпьютер использует процессоры ARM A64FX общей численностью 7630848 ядер и установив новый мировой рекорд – 442 петафлопс на HPL. Суперкомпьютер Fugaku был построен корпорацией Fujitsu и установлен в Центре вычислительных наук RIKEN (R-CCS) в Кобе, Япония.

Суперкомпьютер Summit занимает второе место и принадлежит семейству суперкомпьютеров производства IBM, в которых используются процессоры Power9 и графические процессоры NVIDIA Tesla V100. Система Summit Национальной лаборатории Окриджа имеет высшие награды с результатом HPL 148,6 петафлопс при этом в данном суперкомпьютере используется 2,414,592 ядра IBM POWER9 22C 3,07 ГГц.

Рис. 2. Суперкомпьютер Fugaku

На рис. 2 продемонстрирована фотография суперкомпьютера Fugaku на которой видно, что данный компьютер – «серьёзная машина» которая уже внесла свой вклад в мировые бизнес процессы [3].

В основе данного сложного многомашинного комплекса заложены блейд-системы с использованием ARM A64FX процессоров производства корпорации Fujitsu. Компания Fujitsu до настоящего времени отдавала преимущество серверным платформам на базе процессоров SPARC, то выскажем предположение, что вскоре появятся серверные системы, которые заменят линейку серверов на базе процессоров SPARC, либо их значительно потеснят на рынке.

Учитывая, что Fujitsu Siemens Computers является транснациональной корпорацией, то данные изменения в области применения компьютеров на базе Arm процессоров затронут европейские и азиатские рынки. Подтверждением данной гипотезы служит новость от компании Apple которая выпустила линейку ноутбуков на базе процессора Apple M1в основе которого лежит ARM процессор, а как следствие – появятся новые ноутбуки и рабочие станции на базе архитектуры ARM процессоров.

Формально, уже можно начать подготовку специалистов по проектированию компьютерных систем с использованием процессоров архитектуры на базе ARM.

Список используемых источников

1. Сайт Raspberry Pi Foundation. URL: https://www.raspberrypi.org (дата обращения 29.03.2020).

2. Громов В. В. Микрокомпьютеры и перспективы их развития в современном учебном процессе // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО

2020). IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. С. 242–245.

3. Японский суперкомпьютер Fugaku на ARM-процессорах присоединится к борьбе с COVID-19. URL: https://www.google.com/url?sa=i&url=https%3A%2F%2Fservernews.ru%2F1007824&psig =AOvVaw2ymWTgJ9QhJ_wQeTADAun3&ust =1617654116091000&source =images&cd=vfe&ved=0CAIQjRxqFwoTCIDY_am15e8CFQAAAAAdAAAAABAr

УДК 004.451
ГРНТИ 20.01

ОПРЕДЕЛЕНИЕ ПОРЯДКА ФУНКЦИОНИРОВАНИЯ РАЗРАБАТЫВАЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ХРАНЕНИЯ И ОБМЕНА ЭЛЕКТРОННЫХ КАФЕДРАЛЬНЫХ НАУЧНЫХ МАТЕРИАЛОВ В УСЛОВИЯХ МНОГОПОЛЬЗОВАТЕЛЬСКОГО РЕЖИМА

В. В. Громов, К. Д. Скоробогатов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена определению операционной системы для серверного программного обеспечения, основанного на выбранном стеке технологий: языке программирования Python и системе управления базами данных MariaDB. Содержит результаты синтетического тестирования на сервере и сравнительного анализа самых востребованных современных серверных операционных систем на ядре Linux. Практическое применение результатов исследования позволит грамотно выбрать серверную операционную систему в соответствии с поставленными задачами.

Ubuntu, Debian, CentOS, серверная ОС, синтетическое тестирование.

В рамках работы, направленной на реализацию серверного программного обеспечения для хранения и обмена электронных кафедральных научных материалов, необходимо выбрать соответствующую необходимым требованиям серверную операционную систему. Такая ОС выступит в качестве платформы для запуска разрабатываемого многопользовательского сетевого ПО, из-за особенностей развертывания которого, необходимо выделить ряд основных требований к северной ОС, а именно производительность системы, стабильность, масштабируемость, доступность для тестирования (обладание свободной ли-

цензией), и не менее важное безопасность, так как сервер будет работать с данными – результатами интеллектуальной деятельности студентов, преподавателей и т. п.

В соответствии с требованиями к безопасности и свободному доступу можно выделить популярные дистрибутивы на ядре Linux: Debian, Ubuntu, CentOS и Fedora, а также ОС FreeBSD семейства BSD [1]. Так как FreeBSD не основана на ядре Linux, то проводить её сравнение с Linux-дистрибутивами будет нерационально, а для сопоставления последних, необходимо провести анализ по следующим критериям:

1) Официальная поддержка выбранного ранее технологического стека: Python-интерпретатора и СУБД MariaDB;

2) Поддержка контейнеризации, которая расширяет возможности масштабируемости и изоляции ПО, увеличивает безопасность ПО, снижая поверхность атаки [2];

3) Поддержка процессоров на архитектуре ARM, позволяющих запускать ОС на современных экономически выгодных серверах [3];

4) Срок официальной поддержки.

Результаты анализа представлены в таблице 1, источники [4, 5].

ТАБЛИЦА 1. Анализ Linux и BSD дистрибутивов

ОС	Ubuntu 20.04	Debian 10	CentOS 8	Fedora 32
Поддержка интерпретатора Python	+	+	+	+
Поддержка СУБД MariaDB	+	+	+	+
Поддержка контейнеризации	+	+	+	+
Поддержка процессоров ARM	+	+	+	+
Срок поддержки версии	4 года (до 2024)	5 лет (до 2024)	5 лет (до 2024)	9 месяцев после релиза (до 28 января 2021)

На основе результатов анализа невозможно определить лучшую по параметрам сравнения ОС. Чтобы уйти от неопределенности было принято решение провести синтетическое тестирование. Тестирование проходило на сервере с использованием одинаковой конфигурации оборудования: один процессор Intel Xeon E5, один SSD-диск объемом 20 ГБ (скорость чтения/записи: 340 МБ/с / 230 МБ/с) и ОЗУ на 512 МБ. Тестируемые операционные системы обладали файловой системой ext4.

Для первой части тестирования была написана программа на ЯП Python, фрагмент которого представлен на рис. 1. Скрипт генерировал 900 файлов, каж-

дый из которых обладал размером 977 КБ. Затем происходило заполнение таблицы, чтение записанных данных из заранее подключеной СУБД MariaDB, запись сгенерированных файлов в директорию файловой системы. Время выполнения каждой операции фиксировалось. Тест запускался три раза, в таблице 2 представлены усредненные значения результатов выполнения программы.

```
def time_of_function(function):...
def file_generator(num_of_files, content_size):...

@time_of_function
def write_to_db(curr, files_count_len) :
    cur.execute("DROP TABLE IF EXISTS test0")
    cur.execute("CREATE TABLE test0 (ID INT AUTO_INCREMENT, NAME
VARCHAR(50), ..., CREATION DATE, PRIMARY KEY(ID));")
    for i in range(0, files_count_len):
        cur.execute("INSERT INTO test0 (NAME, ADDINFO, FILEPATH, CREATION)
VALUES (?, ?, ?, ?)",(f"{files_count[i]}", random_string(20),
f"/home/root/test/{files_count[i]}", datetime.datetime.now()))

@time_of_function
def read_from_db(curr, files_count_len):
    cur.execute("SELECT name, addinfo, filepath, creation FROM test0")
    for name, addinfo, filepath, creation in cur:
        pass

@time_of_function
def move_files_to_directory(files_count_len):
    for i in range(0, files_count_len):
        shutil.copy2(f'./files/{files_count[i]}',
f'/home/root/test/new{files_count[i]}')

if __name__ == '__main__':
    file_generator(900, 1000000)
    try:
        conn = mariadb.connect(user="root", password="1234",
host="127.0.0.1", port=3306, database="TESTS")
    except mariadb.Error as e:
        print(f"Error connecting to MariaDB Platform: {e}")
        sys.exit(1)
    cur = conn.cursor()
    files_count = os.listdir(path="./files")
    write_to_db(cur, len(files_count))
    read_from_db(cur, len(files_count))
    move_files_to_directory(cur, len(files_count))
    conn.close()
```

Рис. 3. Фрагмент программы на ЯП Python

ТАБЛИЦА 2. Результаты тестирования

ОС	Ubuntu 20.04	Debian 10	CentOS 8	Fedora 23
Время записи 900 строк данных в БД в секундах	0,12	0,16	0,11	0,16
Время копирования 900 файлов в директорию файловой системы ОС в секундах	8,42	8,01	6,04	6,44
Время чтения 900 записей из БД в секундах	0,04	0,04	0,28	0,004

Как видно из результатов, приведенных в таблице 2, ОС CentOS 8 обладает большим преимуществом по скорости записи данных в БД и времени копирования файлов в директорию файловой системы ОС.

Вторая часть тестирования заключалась в оценке производительности СУБД MariaDB с помощью утилиты sysbench. С помощью первой и второй команды (рис. 1) была сгенерирована таблица на 50 000 записей, создано условие взаимодействия с 8 клиентами (максимальное число запросов 1 000) и запущен сам тест.

```
sysbench --db-driver=mysql --mysql-user=root --mysql-password=1234 --mysql-db=sbtest --table_size=50000
--threads=8 --max-requests=1000 --rand-type=uniform /usr/share/sysbench/oltp_read_only.lua prepare

sysbench --db-driver=mysql --mysql-user=root --mysql-password=1234 --mysql-db=sbtest --table_size=50000
--threads=8 --max-requests=1000 --rand-type=uniform /usr/share/sysbench/oltp_read_only.lua run
```

Рис. 4. Команды подготовки и запуска теста утилиты sysbench

В получившемся отчете наибольшим интересом обладал параметр, связанный с количеством выполненных транзакций в секунду, каждая из которых состояла из запросов на чтение данных. Результаты представлены на рис. 3.

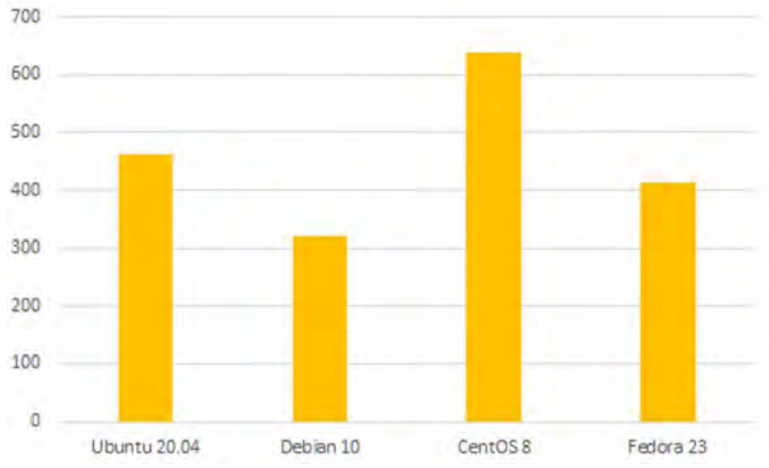


Рис. 5. Количество выполненных транзакций в секунду для СУБД MariaDB

Как видно из результатов тестирования с использованием утилиты sysbench, наибольшая производительность СУБД MariaDB прослеживается на ОС CentOS 8.

В результате синтетических тестов ОС CentOS 8 показала наилучшие результаты почти по всем тестируемым параметрам. Таким образом, для развертывания разрабатываемого ПО для хранения и обмена научных кафедральных материалов будет выбрана серверная ОС CentOS 8.

Список используемых источников

1. Марданов Д. Д., Вахрушева Е. А., Дубовцев И. К. Сравнительный анализ серверных операционных систем // Информационные технологии в науке, промышленности и образовании: сб. тр. Всероссийской науч. техн. конф. / Под. ред. К. Ю. Петухова. Ижевск: Изд-во ИжГТУ им. М. Т. Калашникова, 2019. С. 198–203.

2. Степанов В. В., Плис А. Д., Шостик Н. В. Безопасное построение и совместное использование web-сервера на основе Docker // Морская стратегия и политика России в контексте обеспечения национальной безопасности и устойчивого развития в XXI веке: сб. науч. тр. / Под. ред. В. А. Судакова, Н. Ф. Лазицкой, А. Л. Рябкева, Л. А. Цыбульской, Е. Е. Рябцевой, В. В. Болотовой. Севастополь: ЧВВМУ имени П. С. Нахимова, 2020. Вып 25. С. 269–273.

3. ARM серверы – более производительные и более дешёвые. URL: https://habr.com/ru/post/535792/ (дата обращения 19.03.2021).

4. DistroWatch.com: Put the fun back into computing. URL: https://distrowatch.com/ (дата обращения 19.03.2021).

5. Choosing an OS: CentOS, Ubuntu, Debian, FreeBSD, CoreOS, or Windows Server. URL: https://www.vultr.com/docs/choosing-an-os-centos-ubuntu-debian-freebsd-coreos-or-windows-server (дата обращения 19.03.2021).

УДК 004.93
ГРНТИ 20.53.19

ИССЛЕДОВАНИЕ ИНФОРМАЦИОННОЙ ЭФФЕКТИВНОСТИ ЦИФРОВЫХ СГЛАЖИВАЮЩИХ ФИЛЬТРОВ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время достаточно актуальным является использование информационных оценок в задачах интеллектуального анализа возникновения состояний неопределенности в системах обработки данных различной природы. В работе рассматриваются методы оценки влияния параметров цифровых сглаживающих фильтров на их информационную эффективность при сглаживании аддитивных случайных помех и выделении полезной составляющей входного сигнала. Исследования основаны на анализе изменений энтропии и динамики информационных процессов сглаживания случайных сигналов.

информация, интеллектуальный анализ, фильтрация, Колмогоровская сложность.

В настоящее время достаточно актуальной является использование информационных оценок в задачах интеллектуального анализа возникновения состояний неопределенности в различного рода системах обработки данных. Причиной возникновения состояний неопределенности при сглаживании случайных сигналов является априорная неопределенность по отношению к характеристикам воздействующих на полезный сигнал помех.

В [1] рассмотрены вопросы определения коэффициента информационной эффективности цифровых сглаживающих фильтров, значение которого представить в виде выражения:

$$K_{\text{иэ}} = \frac{ln\frac{\sigma_x}{\sigma_y}}{K(z)},$$

где Колмогоровская сложность фильтра $K(z)$ может рассматриваться как минимальная длина программы, реализующая фильтр z при наличии информации о x и y [2], а σ_x и σ_y – значения среднеквадратических ошибок входного и выходного сигналов соответственно.

Представляет интерес рассмотреть влияние параметров цифрового фильтра на его информационную эффективность.

Пусть осуществляется сглаживание помех и выделение полезной составляющей двумя цифровыми фильтрами с разными характеристиками сглаживания, но обладающими одинаковыми показателями Колмогоровской сложности и обрабатывающими один и тот же входной сигнал *x*, при этом оценка информационной эффективности каждого фильтра представляет собой следующие выражения:

$$K_{\text{иэ1}} = \frac{ln\frac{\sigma_x}{\sigma_{y1}}}{K(z)},\ K_{\text{иэ2}} = \frac{ln\frac{\sigma_x}{\sigma_{y2}}}{K(z)}.$$

Эти выражения позволяют определить показатель Колмогоровской сложности для фильтров как

$$K_1(z) = \frac{ln\frac{\sigma_x}{\sigma_{y1}}}{K_{\text{иэ1}}},\ K_2(z) = \frac{ln\frac{\sigma_x}{\sigma_{y2}}}{K_{\text{иэ2}}}.$$

Определим $K_{\text{иэ2}} = K_{\text{иэ1}} + \Delta K_{\text{иэ1}}$, и учитывая равенство показателей Колмогоровской сложности для рассматриваемых фильтров можно записать, что

$$\frac{ln\frac{\sigma_x}{\sigma_{y1}}}{K_{\text{иэ1}}} = \frac{ln\frac{\sigma_x}{\sigma_{y2}}}{K_{\text{иэ1}}+\Delta K_{\text{иэ}}}\ .$$

Из последнего выражения следует

$$ln\frac{\sigma_x}{\sigma_{y1}}(K_{\text{иэ1}} + \Delta K_{\text{иэ}}) = K_{\text{иэ1}} ln\frac{\sigma_x}{\sigma_{y2}},$$

и далее

$$ln\frac{\sigma_x}{\sigma_{y1}}(1 + \frac{\Delta K_{\text{иэ}}}{K_{\text{иэ1}}}) = ln\frac{\sigma_x}{\sigma_{y2}}\ ,$$

откуда

$$\frac{\Delta K_{\text{иэ}}}{K_{\text{иэ1}}} = \frac{ln\frac{\sigma_{y1}}{\sigma_{y2}}}{ln\frac{\sigma_x}{\sigma_{y1}}}.$$

Полученное выражение позволяет оценить относительное изменение значения коэффициента информационной эффективности цифровых сглаживающих фильтров в зависимости от изменений их параметров.

Пример. Рассмотрим процесс сглаживания аддитивной некоррелированной помехи рекурсивным цифровым фильтром, передаточная функция которого имеет следующий вид:

$$\Phi(z) = \frac{0{,}5b_0(z+1)}{(z-j)^2},$$

где $b_0 = (1 - j)^2$ при $|j| < 1$, а z – аргумент z-преобразования.

Для данного класса фильтров обеспечивается снижение уровня помех до оптимальных значений дисперсии случайной ошибки на выходе фильтра [3]:

$$\sigma^2 = \frac{0{,}5(1-j)}{1+j},$$

где $\sigma = \frac{\sigma_y}{\sigma_x}$, σ_x, σ_y – СКО на входе и выходе цифрового фильтра соответственно.

Без потери общности можно предположить, что $\sigma_x = 1$.

Тогда, определив значение нулей характеристического полинома для первого фильтра $j_1 = j_2 = 0{,}96$, при которых

$$\sigma_{y1} = \sqrt[2]{0{,}010} = 0{,}1,$$

и изменяя значения $j_1 = j_2$, для второго фильтра можно получить зависимость относительного изменения значения коэффициента информационной эффективности для второго фильтра (рис.) при заданных условиях.

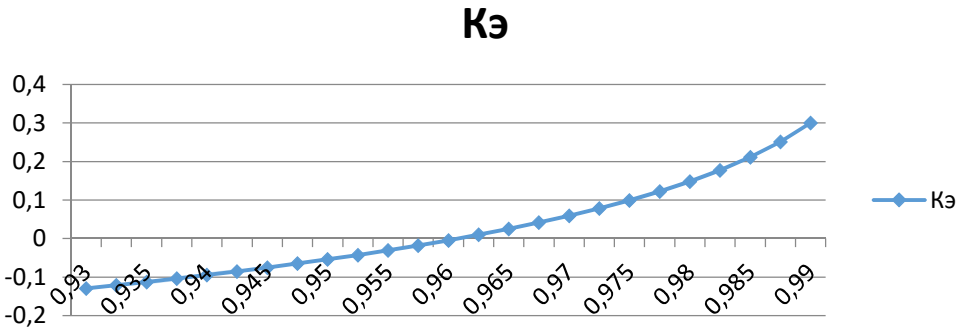


Рис. Зависимость изменения значений относительного коэффициента информационной эффективности для цифрового фильтра

Список используемых источников

1. Губин А. Н., Литвинов В. Л., Филиппов Ф. В. Оценка информационной эффективности устройств цифровой обработки информации // XXIII Международная конференция по мягким вычислениям и измерениям (SCM-2020). Сборник докладов. Санкт-Петербург. 27–29 мая 2020 г. СПб.: СПбГЭТУ «ЛЭТИ», 2020. С. 8–10.

2. Колмогоров А. Н. Три подхода к определению понятия «Количество информации» // Новое в жизни, науке, технике. Сер. «Математика, кибернетика». 1991. № 1. С. 24–29.

3. Губин А. Н. О выборе параметров при синтезе оптимальных операторов обработки цифровой информации в АСУ ТП // В сб. Проблемы системотехники и АСУ. Л.: СЗПИ, 1981. С. 137–141.

УДК 004.891.2
ГРНТИ 20.23.17

ПРИМЕНЕНИЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Обслуживание и сопровождение информационных систем осуществляется службами технической поддержки. С расширением поддерживаемой инфраструктуры возрастает нагрузка на службу поддержки, увеличивается численность специалистов, применяются специальные методологии и инструменты управления поддержкой. В настоящее время наибольший интерес вызывают интеллектуальные системы поддержки принятия решения, которые ассистируют лицам, принимающим решения, в принятии этих решений, используя нейросетевые инструментарии. В работе предложены современные подходы на базе методов обработки текстов на естественном языке (Natural Language Processing, NLP).

интеллектуальные системы поддержки принятия решений, обработка текстов на естественном языке, NLP.

Работа службы технической поддержки ежедневно связана с обработкой десятков и сотен заявок, поступающих от пользователей обслуживаемых информационных систем. Прежде, чем заявка будет выполнена, она должна пройти определенный маршрут, чтобы получить назначение на специалиста, ответственного на выполнение данной заявки. Чем больше пользователей информационных систем, тем сложнее структура самой службы поддержки, а значит и сложнее маршрут заявки от заказчика к исполнителю. Неверные решения на каждом этапе эскалации могут привести к затягиванию сроков выполнения заявки, простою бизнеса и убыткам.

Таким образом, с ростом накопленной информации о поступающих заявках и показателях работы операторов технической поддержки появляется необходимость автоматизации процесса маршрутизации. Для уменьшения рисков принятия неверного решения может быть предложено внедрение интеллектуальной системы поддержки принятия решений. Использование интеллектуальных систем поддержки принятия решений позволяет сократить сроки обработки заявок, увеличить скорость их маршрутизации без ущерба качеству работы технической поддержки [1, 2].

Для функционирования данных служб разработаны методологии, специализированные информационные системы класса Service Desk. При этом даже

полное следование методологии ITIL (методология управления, отладки и непрерывного улучшения бизнес-процессов, связанных с информационными технологиями) не может уберечь от принятия неверного решения, а в большинстве систем класса Service Desk полностью отсутствует функционал для поддержки принятия решений, будь то заведение обращения пользователем, первичная обработка обращения специалистом поддержки или сопровождение дальнейшего жизненного цикла заявки, вплоть до предоставления окончательного решения заказчику.

Концепция использования интеллектуального анализа текста в интеллектуальной системе поддержки принятия решения [3, 4] службы технической поддержки состоит в классификации входящих обращений пользователей путём анализа описания инцидента. При сопоставлении текста нового обращения с базой данных архивных обращений, которые уже были категорированы и апробированы специалистами поддержки, ИСППР определяет вероятную категорию для нового обращения и предлагает данную категорию пользователю или специалисту, приступившему к обработки данного обращения. При этом технология интеллектуального анализа текста не должна быть ресурсоёмкой в процессе эксплуатации, так как количество обращений в данную службу поддержку постоянно возрастает и длительное время обработки повлечет отрицательный рост качества оказываемых услуг.

На рис. 1 представлен жизненный цикл заявки в службу технической поддержки информационной системы регионального уровня. Использование интеллектуального анализа текста возможно на этапе регистрации заявки пользователем через веб-интерфейс системы класса GLPI (*Gestionnaire libre de parc informatique*, Свободный менеджер ИТ-инфраструктуры), а также при выборе категории специалистом первой линии поддержки. Апробация предоставленного решения и корректной категории (как показано в таблице) происходит на этапе закрытия заявки, после чего она попадает в архив, на основании которого может происходить дальнейшее обучение модели.

Работа службы поддержки информационной системы строится на обработке и выполнении поступающих заявок. Заявки поступают от пользователей информационной системы в информационную систему класса Service Desk GLPI. Алгоритм работы модуля векторного представления документов представлен на рис. 2.

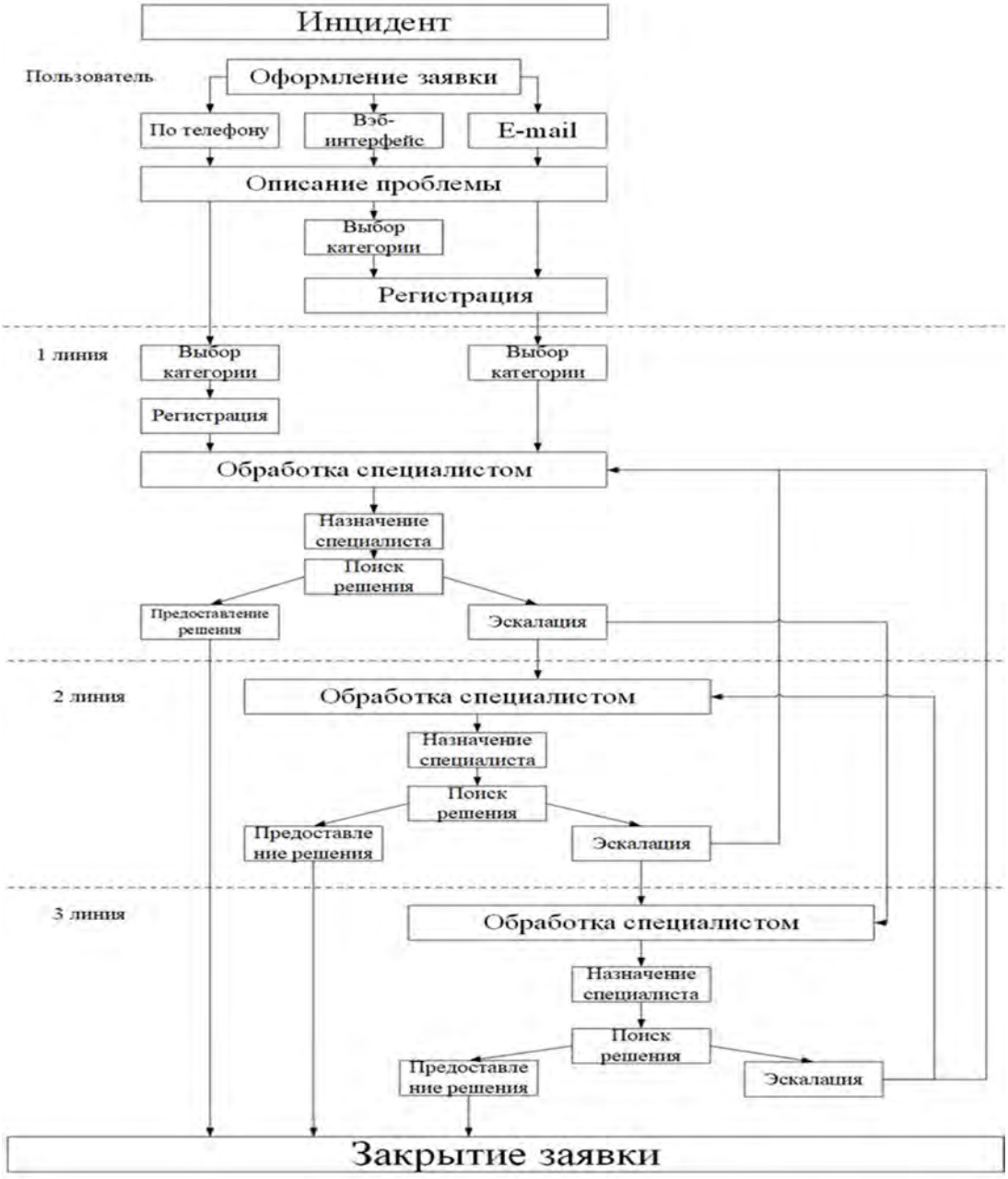


Рис. 1. Жизненный цикл заявки

Интеллектуальная система поддержки принятия решения представляет из себя модуль расширения к системе класса Service Desk. ИСППР должна предлагать решение на следующих этапах:

1. Выбор категории пользователем при оформлении заявки через веб-интерфейс. При регистрации заявки необходимо указать корректную категорию для корректной маршрутизации заявки. При этом значение поля «Описание» записывается в базу данных системы Service Desk только после регистрации заявки и создания тикета. В этот момент времени в работу должен включиться модуль векторного представления документов. На вход данного модуля пода-

ётся описание заявки. После обработки и сравнения данного документа с моделью формируется вероятно корректная категория для этого тикета и предлагается пользователю через веб-интерфейс. Пользователь должен согласовать и принять это решение, либо изменить категорию по своему усмотрению.

2. Обработка заявки специалистом службы поддержки. При обработке заявки специалистом службы поддержки в работы также включается модуль векторного анализа документов, который, анализируя текст описания заявки, предлагает корректную и семантически близкую категорию. Специалист вправе согласовать изменение категории, изменить ее самостоятельно или оставить категорию, выбранную пользователем без изменений. На странице «Решение» по каждой заявке модуль векторного представления документов на основе анализа описания и категории заявки предлагает специалисту службы поддержки одно из апробированных решений по данной категории заявок, которое специалист также вправе одобрить или выбрать/описать самостоятельно.

ТАБЛИЦА. Сопоставление текстов входящего документа и документа из модели

Входящий документ	Документ из модели	Корректно ли сопоставление категорий
Выдает ошибку при добавлении внутреннего адресата	После регистрации проекта документа при отправке адресату не проставили дату, в связи чем документ не доходит до адресата.	Корректно
Ошибка при выполнении запроса. Оператор не имеет права на вызов сервиса.	Не подтверждены учётные записи.	Корректно
В какую папку попадают проекты резолюций?	Не отображаются поступившие документы. Просмотренные документы определяются как вновь входящие.	Корректно
Счетная палата. Проблемы с подключением принтера.	Замена расходных материалов в оргтехнике.	Корректно
ИБП не работает	Установка и настройка информационных систем.	Не корректно
Добрый день! Не удается войти в программу со своей учетной записи.	Не дает зайти в программу.	Корректно
В услуге "Оказание адресной социальной поддержки в возмещение расходов…" в тех структурных подразделениях, где добавлена данная услуга, необходимо внести изменения в форму.	Управление почтовыми ящиками пользователей.	Не корректно
Доброе утро! Специалист не может войти в компьютер.	Отключился компьютер, погас экран.	Не корректно

Входящий документ	Документ из модели	Корректно ли сопоставление категорий
Добрый день! В связи со служебной необходимостью прошу установить на компьютер Bitrix 24 Desktop.	Установить справочник.	Корректно

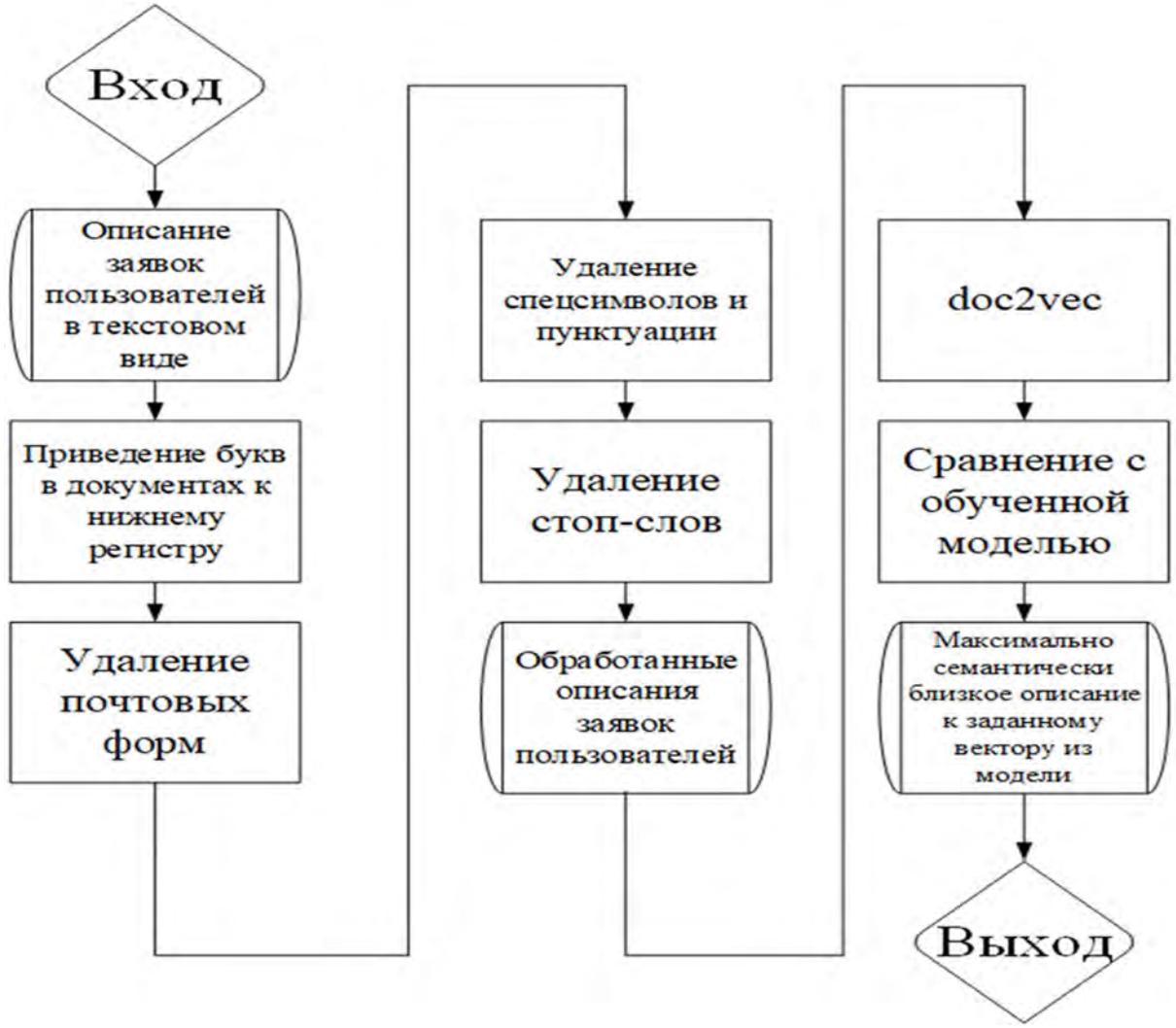


Рис. 2. Алгоритм работы модуля векторного представления документов

В процессе тестирования алгоритма выявлено успешное сопоставление документов на уровне в 85 %. При исследовании ИСППР в имитационной среде AnyLogic продемонстрированы результаты, способствующие снижению нагрузки на отдел, а также уменьшение времени ожидания пользователей в связи с уменьшением длины очереди.

Список используемых источников

1. Попов А. Л. Системы поддержки принятия решений: учебно-метод. пособие. Екатеринбург: Урал. гос. ун-т, 2008. 80 с.

2. Интеллектуальные системы поддержки принятия решений – краткий обзор. URL: https://habr.com/ru/company/ods/blog/359188/ (дата обращения 30.01.2021).

3. Litvinov, V. L. Research of Neural Network Methods of Text Information Classification. 2019 III International Conference on Control in Technical Systems (CTS). 30 Oct.–1 Nov. 2019. doi: 10.1109/CTS48763.2019.8973314.

4. Komarovskikh, D. O.; Litvinov, V. L. Research of a recurrent neural network for the vector representation of nucleotide sequences. 2020 XXIII International Conference on Soft Computing and Measurements (SCM). 27–29 May 2020. doi: 10.1109/SCM50615.2020.9198757.

УДК 004.852
ГРНТИ 28.23.37

ПРОЦЕДУРЫ ВАРИАЦИОННОГО ПУЛИНГА ДЛЯ МОДЕЛИРОВАНИЯ СЕТЧАТКИ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Предложены процедуры моделирования латеральных связей в сплетениевидных слоях. В основу построения моделей положен принцип использования неравномерной субдискретизации. Исследования основаны на анализе функционирования горизонтальных и амакриновых клеток сетчатки глаза с точки зрения машинного моделирования. Предложенные модели могут найти свое применение в новых нейросетевых архитектурах.

компьютерное зрение, сетчатка глаза, нейронные сети, пулинг.

Наружный сегмент фоторецепторов сетчатки глаза человека включает порядка 120 млн. палочек и 6 млн. колбочек, хотя лишь около 1,2 млн волокон формируют зрительный нерв. Таким образом, в сетчатке выполняется большой объем предварительной обработки сенсорной информации, снижающей размерность анализируемых данных более, чем в 100 раз. Совершенство зрительного аппарата человека дает основание предположить, что чем точнее удастся смоделировать реальные процессы обработки, тем более эффективной будет модель. В связи с этим, в работе делается попытка исследовать процесс обработки и передачи сигналов от фоторецепторов до волокон зрительного нерва.

Рассмотрим упрощенную структуру сетчатки глаза, достаточную для пояснения идеи предлагаемых гипотез и процедур моделирования [1]. Нейронная сеть сетчатки включает 4 типа нервных клеток: *ганглионарые (ганглиозные)*, *биполярные*, *амакриновые* и *горизонтальные* клетки (рис. 1).

Ганглионарные клетки – это нейроны, аксоны которых в составе зрительного нерва выходят из глаза и следуют в центральную нервную систему, именно их количество оценивается примерно в 1,2 миллиона.

Биполярные клетки соединяют фотоцепторы и ганглиозные клетки. От тела биполярной клетки отходят два разветвленных отростка: один отросток образует синаптические контакты с несколькими фоторецепторными клетками, другой – с несколькими ганглиозными клетками. Функция биполярных клеток – проведение возбуждения от фоторецепторов к ганглиозным клеткам. Кроме палочек и колбочек, биполяры также имеют связи с горизонтальными клетками. То есть биполяры прибегают как к прямому, так и косвенному пути передачи сенсорной информации в сетчатке.

Горизонтальные клетки соединяют расположенные рядом фоторецепторы. От тела горизонтальной клетки отходит несколько отростков, которые образуют синаптические контакты с фоторецепторами. Основная функция горизонтальных клеток – осуществление латеральных взаимодействий фоторецепторов.

Амакриновые клетки расположены подобно горизонтальным, но их образуют контакты не с фоторецепторными, а с ганглиозными клетками.

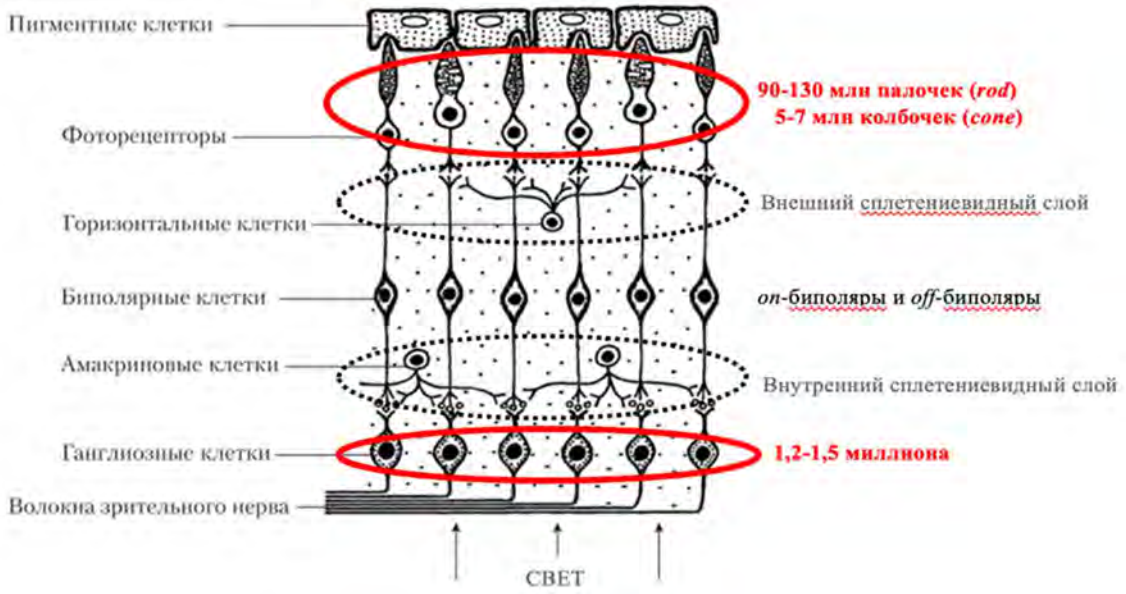


Рис. 1. Структура сетчатки глаза

Клетки сетчатки связаны между собой сложной сетью возбуждающих, подавляющих и двунаправленных сигнальных связей. Они собирают информацию от всех слоев сетчатки как по вертикальным путям: фоторецепторы – биполяры - ганглионарные клетки, так и по латеральным путям: горизонтальные клетки – биполяры – амакриновые клетки [2, 3].

Попытаемся формализовать приведенную выше информацию для построения структурной модели нейронной сети сетчатки. Прежде всего следует подчеркнуть, что задача, решаемая сетчаткой, существенно отличается от тех задач, которые решаются «классическими» нейронными сетями. Главная цель состоит в реализации сюръективного отображения множества элементов входа (фоторецепторного слоя) во множество элементов выхода (волокна зрительного нерва). При этом необходимо обеспечить пропорциональное масштабирование (пулинг) исходного изображения в среднем с коэффициентом 1/100. Очевидно, эта задача решается поэтапно, каждый слой нервных клеток сетчатки выполняет свою задачу.

Рассмотрим возможные варианты *моделирования работы слоя горизонтальных клеток*. Фоторецепторы размещаются в сетчатке очень плотно, в виде шестиугольников (гексагональная упаковка). На рис. 2, слева представлена модель центральной части структуры слоя фоторецепторов. Если обозначить минимальный шестиугольник состоящий из 7 фоторецепторов за k_1, то количество фоторецепторов в гексагональной упаковке, отстоящей от центра на n элементов, можно оценить с помощью рекуррентной формулы:

$$k_n = k_{n\text{-}1} + 6n.$$

Масштабирование можно осуществлять на уровне минимальных связанных элементов структуры, как это показано на рис. 2, справа. Очевидно, что пропорциональность возможно будет обеспечить только в случае учета изменений свойств на уровне ближайших соседей, что и выполняется в слое горизонтальных клеток. Этот, так называемый внешний пулинг, основанный на использовании модели латерального торможения.

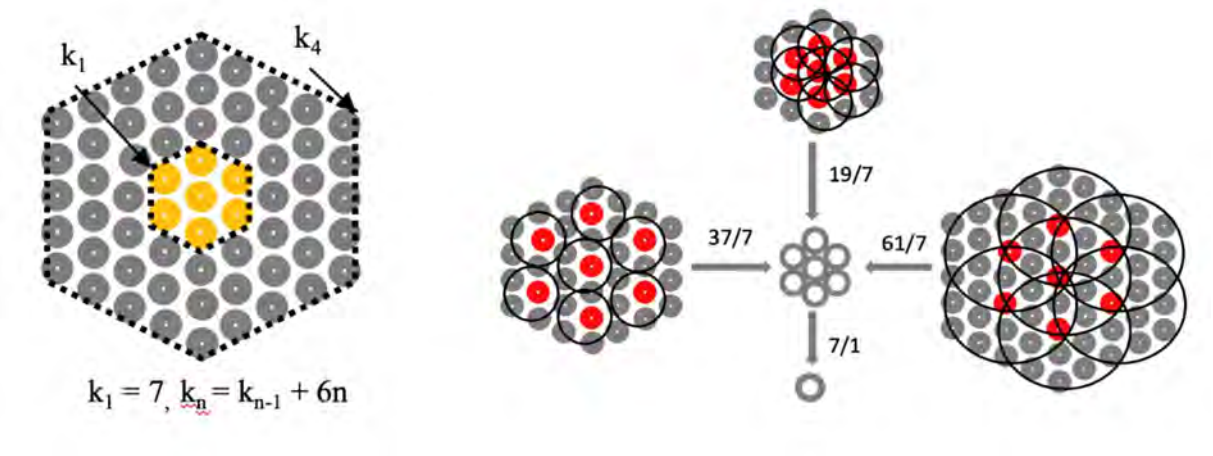


Рис. 2. Модель структуры слоя фоторецепторов

Следует пояснить, что в качестве модели клетки горизонтального слоя будем рассматривать нейрон, имеющий три вектора взаимодействия с окружающей средой – входной, вход-выходной и выходной (рис. 3).

Рис. 3. Модель горизонтального нейрона

Начальное состояние горизонтального нейрона устанавливается равным (эквивалентным) уровню «серого» входного фоторецептора. В процессе функционирования модели сетчатки состояние изменяется в соответствии с реализацией процесса латерального торможения.

Для управления процессом латерального торможения удобно ввести понятие порога торможения Δ, который задается величиной:

$$\Delta = (s_1 - s_2)/100,$$

где s_1 и s_2 состояния соседних горизонтальных клеток. Порог будет определять предельное значение разности активаций соседних горизонтальных клеток, при котором обе клетки будут принадлежать одной эквипотенциальной зоне слоя горизонтальных клеток. Если не накладывать никаких дополнительных условий, то есть Δ = 0 – порог максимального латерального торможения – эквипотенциальные зоны будут образованы нейронами с одинаковыми состояниями. При этом будет обеспечено максимально точное пропорциональное масштабирование.

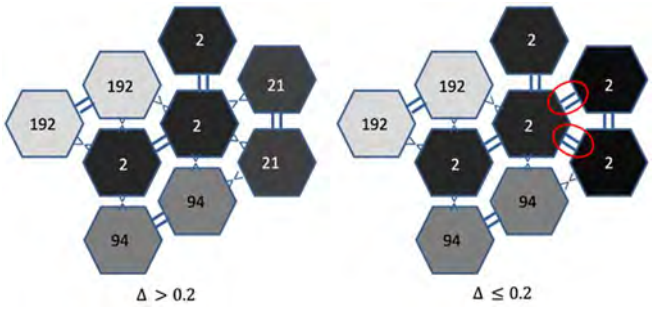


Рис. 4. Изменение эквипотенциальных зон при изменении порога

Поскольку точное количество фоторецепторов и горизонтальных клетках неизвестно, введение порога торможения позволит осуществлять эксперименты, приближающие опыты к реальным наблюдаемым данным. На рис. 4 показан пример изменения эквипотенциальных зон при задании порога Δ = 0,2. Возможность слияния определяется состоянием вход-выходного вектора соответствующей пары нейронов. На рис. 4 эта возможность отображается знаком «=». В этом случае две пары соседних клеток становятся «эквивалентными» и они сливаются в одну эквипотенциальную зону.

Таким образом, слой горизонтальных клеток выполняет задачу формирования сюръективного отображения с любым, наперед заданным порогом торможения. В результате формируется карта эквипотенциальных зон, на основе

которой производится дальнейший пулинг. Следует отметить, что формирование эквипотенциальных зон необходимо осуществлять с учетом концентрической структуры рецептивных полей. Для этой цели можно применять посекторную обработку, которая допускает расширение радиуса полей при перемещении от центра к периферии.

Рассмотрим возможные варианты *моделирования* пулинга с использованием слоя биполярных нейронов. Задачей этого этапа является масштабирующий перенос сформированной карты эквипотенциальных зон на внутренний слой амакриновых нейронов. Здесь биполяры выполняют две специфические функции: формирование границ эквипотенциальных зон на внутреннем слое и назначение уровня «серого» для каждой эквипотенциальной зоны. Упомянутый масштабирующий перенос по сути осуществляет копирование карты эквипотенциальных зон на шаблоны сформированные на внутреннем слое. Известно, что здесь присутствует три типа рецептивных полей – узкие (70 мкм), средние – (170 мкм) и широкие (350 мкм), расположенные в соответствии с пропорциональным распределением вертикальных (межслойных) и горизонтальных (внутрислойных) связей [4, 5]. Известно, что вертикальные связи, образуемые биполярами проходят неравномерно. В зоне центра, для обеспечения высокого разрешения их концентрация велика, в то время, как по направлению к периферии заметно снижается.

Вертикальные связи биполяров определяют границы соответствия эквипотенциальных зон внешнего слоя горизонтальных клеток с шаблонами, составленными из рецептивных полей внутреннего слоя. Здесь используются отличительные свойства on- и off-биполяров формирования границ переходов.

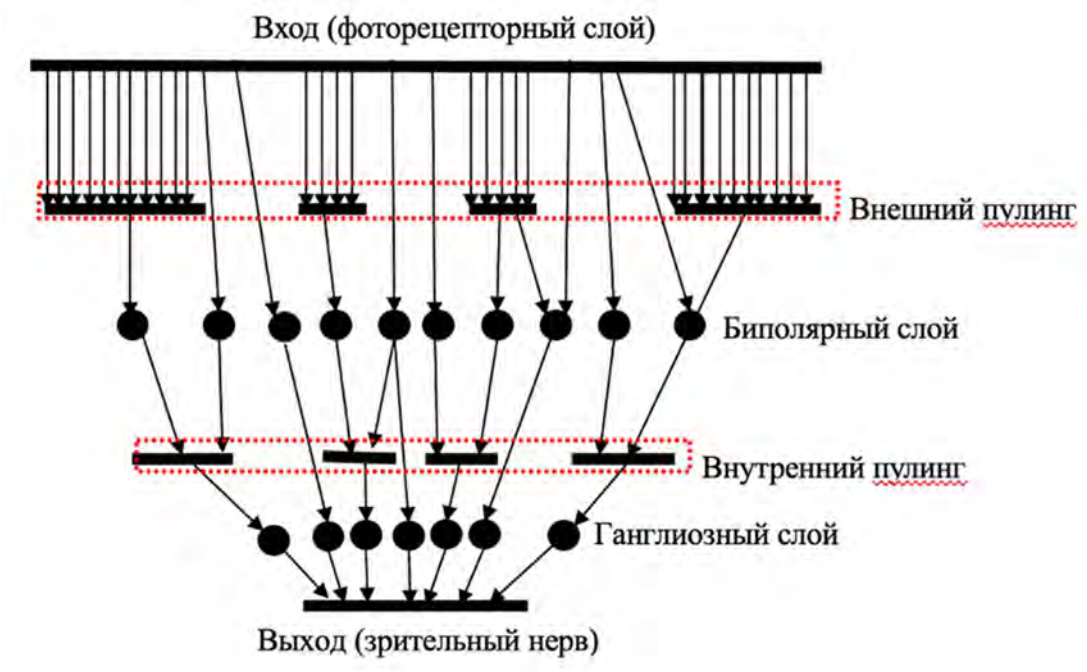


Рис. 5. Архитектура сети моделирования сетчатки

В результате, предлагаемая общая архитектура нейронной сети для моделирования работы слоев сетчатки может быть представлена в виде рис. 5. Основная работа в реализации сюръективного отображения входа во множество элементов выхода выполняется в слоях внешнего и внутреннего пулинга.

Список используемых источников

1. Сандаков Д. Б. Курс лекций по физиологии. URL: https://www.studmed.ru/sandakov-db-kurs-lekciy-po-fiziologii_a0aa2842c20.html (дата обращения 29.03.2021).

2. Мозг, познание, разум: введение в когнитивные нейронауки : в 2 т. Т. 1 / под ред. Б. Баарса, Н. Гейдж ; пер. с англ. ; под ред. проф. В. В. Шульговского. М. : Лаборатория знаний, 2021. 552 с.

3. Николлс Д., Мартин Р., Валлас Б., Фукс П. От нейрона к мозгу / пер. с англ. П. М. Балабана, А. В. Галкина, Р. А. Гиниатуллина, Р. Н. Хазипова, Л. С. Хируга. М.: Едиториал УРСС, 2003. 672 с.

4. Бондаренко М. Каково разрешение человеческого глаза. URL: https://habr.com/ru/post/468653/ (дата обращения 29.03.2021).

5. Фотографические параметры человеческого глаза. URL: https://www.fotovision.ua/post-27-aspx/ (дата обращения 29.03.2021).

УДК 004.5
ГРНТИ 20.53.01

МЕТОД ВИЗУАЛИЗАЦИИ РЕЗУЛЬТАТОВ UX-ТЕСТИРОВАНИЯ ИНФОРМАЦИОННОГО РЕСУРСА

Е. В. Гунина, С. В. Иванова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье анализируются технологии юзабилити-тестирования eye-tracking и mouse-tracking и методы визуализации результатов UX-тестирования информационного ресурса. Представлено исследование, которое позволяет выявить зависимость между отслеживанием траектории движения глаз пользователя, передвижением курсора мыши и сделанными пользователем клики. Актуальность данного исследования состоит в том, что методы визуализации UX-тестирования позволяют качественно анализировать внешний вид страницы сети Интернет и навигацию по ним с целью повышения юзабилити, и существует необходимость более детально рассмотреть данные методы с целью дальнейшего практического применения. Рассмотрена возможность создания нового метода визуализации результатов юзабилити-тестирования.

mouse-tracking, eye-tracking, UX-тестирование, визуализация результатов, юзабилити.

В настоящее время информация по всему миру в Интернете постоянно возрастает, как и возрастает количество веб-ресурсов. Их посещают тысячи интернет-пользователей в сутки. Но не каждая веб-страница обладает высокой степенью юзабилити и, следовательно, возможности стать популярными и удобными для посетителя резко сокращаются. В целях предотвращения данной проблемы требуются изменения в области навигации и дизайна, для этого необходимо проанализировать методы анализа юзабилити веб-страниц.

Цель статьи – проанализировать технологии mouse- и eye-tracking, а также методы визуализации результатов UX-тестирования информационного ресурса и рассмотреть возможность создания нового метода визуализации результатов юзабилити-тестирования.

Задачи исследования:

1) Проанализировать технологии eye- и mouse-tracking;

2) Рассмотреть методы визуализации результатов UX-тестирования информационного ресурса;

3) Провести исследование на выявление зависимости между отслеживанием пути движения глаз тестируемого, передвижением курсора мыши и сделанными им клики;

4) Рассмотреть возможность создания нового метода визуализации результатов юзабилити-тестирования.

Объектом исследования является юзабилити-тестирование информационного ресурса.

Предметом исследования является визуализация результатов юзабилити-тестирование информационного ресурса.

Актуальность исследования состоит в том, что методы визуализации UX-тестирования предоставляют возможность качественно проводить изучение дизайна веб-страницы и навигации по ней для того, чтобы увеличить юзабилити веб-сайта, и существует необходимость детально рассмотреть данные методы с целью дальнейшего практического применения.

На данный момент имеется большое количество разного рода методов анализа, которые помогают качественно анализировать навигацию по странице и ее дизайн. Представителями таких методов являются mouse- и eye-tracking.

Для проведения исследования на эффективность расположения элементов на веб-сайте и навигации по ней применяется технология eye-tracking, которая изучает поведение тестируемых для того, чтобы увеличить качество и полноту восприятия информации и как следствие, эргономики и экономической отдачи от веб-ресурса [1].

Рис. 1а представляет карту интенсивности, на которой представлено цветовое пространство веб-страницы. Зоны красного цвета посетитель рассматривает с особым интересом и продолжительнее всего, часто возвращаясь к ним. Рис. 1б показывает карту хронологий, из которой видно очередность изучения веб-страницы и длительность остановки взгляда на отдельной детали сайта.

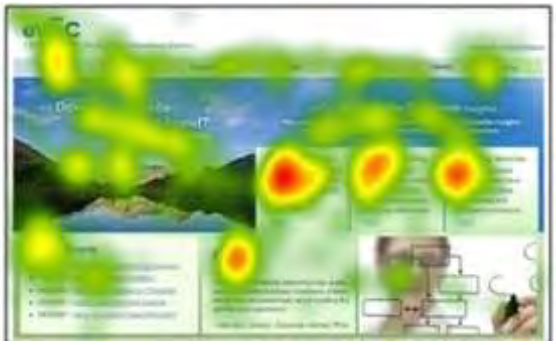
а)  б) 

Рис. 2. а) карта интенсивности, б) карта хронологии

Проведенные опыты с технологией eye-tracking показывают, что прежде всего посетитель осматривает верхнюю и верхнюю левую части веб-страницы и спустя некоторое время знакомится с нижней и правой частями. Из этого следует, что область внимания посетителей представляет собой букву «F». Наиболее важные элементы веб-страницы должны находиться в этих ключевых областях [2].

Вместе с тем технология eye-tracking может эффективно использоваться исключительно для достаточно больших исследований, там, где время и стоимость анализа сравнимы с ожидаемым результатом от использования, так как данная технология сложна и трудоемка в применении и требует наличие определенного оборудования [1].

Технология mouse-tracking позволяет отследить всевозможные действия посетителя, например, переходы, клики по веб-сайту и т. п. Mouse-tracking как методика с самого начала включает в себя недостаток, так, например, в отличие от eye-tracking, в котором расположение взгляда посетителя определяется точно, позиция курсора мыши может отличаться от взгляда пользователя. Независимо от этого, данные, собранные таким способом, требуют большего изучения.

Тепловая карта (*heatmap*) (рис. 2а) показывает распределение кликов посетителей. Карта кликов (рис. 3б) позволяет увидеть нажатия по активным элементам, например: кнопки, ссылки и т. д. Обычно карта кликов представляется в формате точек, мест пересечений или других обозначений для нажатий посетителя.

Анализируя все преимущества технологии mouse-tracking, нельзя не выделить его существенный недостаток, исследование с помощью этой технологии можно будет провести только после его запуска. Но если проект получает дальнейшее развитие, то такая аналитика позволит увеличить эффективность его работы как на новых, так и на постоянных посетителях веб-ресурса [3].

а)  б) 

Рис. 3. а) тепловая карта, б) карта кликов

В научной работе [4], в которой проводилось изучение вопроса о корреляции между движением мыши и взглядом человека, сообщается о точной зависимости курсора и взглядом (около 86 %). Но у данной публикации имеются неточности.

Во-первых, в статье утверждается, что вероятность будет равна 84 %, если в какой-нибудь области веб-страницы была мышь, то пользователь ресурса глядел в то место (даже если в другое время), и вероятность будет равна 88 %, если человек в какую-нибудь область не смотрел, то и мышь там тоже отсутствовала. Однако из того, что посетитель вглядывался в ту область, где была мышь совсем не следует, что курсор был в том месте, куда вглядывался посетитель. Тепловая карта курсора отражает некоторую часть того, что тестируемый, предположительно, увидел.

Во-вторых, невозможно оценить временные параметры восприятия информации по передвижению курсора, в том числе порядок этого восприятия.

В-третьих, данный анализ проводился в 2000 году, когда веб-сайты не были настолько распространены, а посетители – менее опытны.

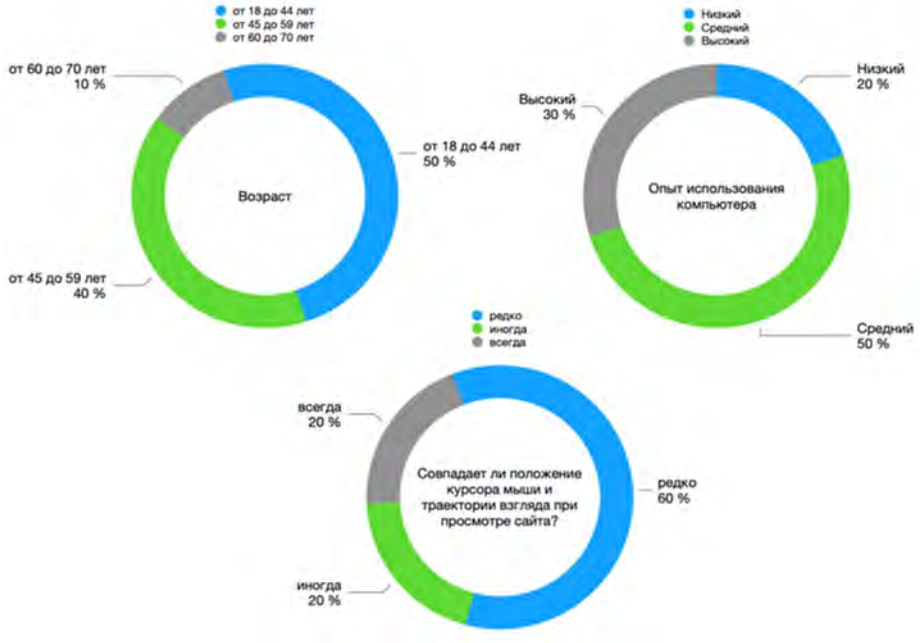
Для проведения исследования на выявление зависимостей между отслеживанием траектории движения глаз пользователя, передвижением курсора мыши и сделанными пользователем клики необходимо выбрать 10 пользователей. Якоб Нильсен в своей статье [5] утверждает, что для проведения тестов достаточно от 5 до 10 человек.

На рис. 3а представлены вопросы для проведения исследования.

Из рис. 3б с результатами исследования видно, что корреляция взгляда и курсора уменьшается с увеличением опыта использования компьютера. В шести случаях из десяти посетители с опытом в основном не передвигают курсор до тех пор, пока не обнаружат взглядом то, на что хотят нажать или прокрутить страницу вниз или вверх; у людей с меньшим опытом подобное поведение встречается в среднем в трех случаях из десяти. Случаи с более или менее точным следованием мыши за взглядом составляет один из десяти, намного реже

предыдущих случаев. И, приблизительно каждый десятый посетитель веб-сайта передвигает курсор совершенно не там, где находится его взгляд.

а)



б)

Рис. 4. а) вопросы для проведения исследования, б) результаты исследования

Частично данное исследование подтверждается более поздними исследованиями корреляции взгляда и курсора:

– 69 % в эксперименте 2005 года [6];
– 42 % в эксперименте 2007 года Google [7];
– 32 % в эксперименте 2008 года Google [8].

Новее исследования не проводились.

В данных случаях проценты корреляции на практике оказались ниже, чем в исследовании [4].

Определенное объединение технологий и методов визуализации результатов тестов mouse- и eye-tracking дает возможным признать создание новой методики в области анализа дизайна и навигации по веб-странице. Тепловые карты обеих технологий (с градацией от теплого цвета к холодному) можно соединить в одну единственную тепловую карту, которая смогла бы показать сумму регистраций взглядов и кликов пользователей. Данный способ даст возможность установить зоны наибольшего внимания посетителей веб-сайта и понять разницу между зрительным и тактильным восприятием информации.

В данном случае имеет место и объединение карт очередности кликов и взглядов. Такого типа аспект вероятно потребует большего анализа из-за сложности восприятия информации, которая связана с увеличением числа регистраций кликов и взглядов. Также имеет важность выявление зависимости между кликом на элементы и длительностью взгляда посетителя на элемент.

Перечисленные подходы помогут установить ранее неизвестные закономерности действий посетителей в целях последующего успешного применения в сфере дизайна, маркетинга и т. д.

Предполагается, что представленный метод приведет к более детальной и эффективной аналитики дизайна веб-страниц.

Список используемых источников

1. Что такое технология «eye-tracking» и как ее использовать? URL: http://siteactiv.ru/about/faq/Eye-tracking_technology (дата обращения 01.02.2021).

2. 23 важных вывода из результатов eye-tracking исследований? URL: http://designformasters.info/posts/23-lessons-from-eye-tracking-studies/ (дата обращения 01.02.2021).

3. Курс: «Информационные технологии» // Mouse-Tracking. URL: wiki.auditory.ru (дата обращения 01.02.2021).

4. What can a mouse cursor tell us more?: correlation of eye/mouse movements on web browsing. URL: https://dl.acm.org/doi/10.1145/ 634067.634234 (дата обращения 01.02.2021).

5. Пять пользователей – все, что нужно для теста. URL: http://www.webmascon.com/topics/testing/4a.asp (дата обращения 01.02.2021).

6. Cooke mouse eye tracker. URL: https://stcsig.org/sn/pdf/cooke_mouse_eye_tracker.pdf (дата обращения 01.02.2021).

7. Исследования Google. URL: http://ryenwhite.com/proceedings/wisi2007.pdf. дата обращения 01.02.2021.

8. Eye-Mouse Coordination Patterns on Web Search Results Pages. URL: http://static.googleusercontent.com/media/ research.google.com/ru//pubs/archive/34367.pdf (дата обращения 01.02.2021).

УДК 004
ГРНТИ 14.85.09

АНАЛИЗ СРЕДСТВ СОЗДАНИЯ ИНТЕРАКТИВНЫХ ЭЛЕМЕНТОВ МУЗЫКАЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ ОБУЧЕНИЯ ИГРЫ НА РАЗЛИЧНЫХ ИНСТРУМЕНТАХ

Е. В. Гунина, Д. Б. Рождественский

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье исследуются средства создания интерактивных элементов приложения для обучения игры на различных инструментах. Дается краткое описание создания и работы интерактивных элементов в различных программах. В ходе изучения материала проводится сравнительный анализ средств и методов разработки, выявляются положительные и отрицательные стороны данных разработок. В результате исследования современных источников информации можно выделить несколько наиболее популярных, а также часто используемых средств разработки интерактивных элементов.

приложение, виртуальная реальность, интерактивный элемент.

В мире много творческих людей, которые хотят реализовать свой потенциал в различных творческих сферах деятельности. Интернет является мощнейшим инструментом для решения таких задач.

Актуальность данной темы связана с необходимостью анализа возможных вариантов создания интерактивных элементов, которые впоследствии могут быть использованными для разработки удобного способа взаимодействия преподавателя и ученика в режиме дистанционного обучения. Наличие интерактивных элементов поможет пользователю увеличить скорость своего обучения, а возможность конструирования более гибких интерактивных элементов позволит преподавателю лучше выстраивать свою образовательную программу, которая зависит от индивидуальных возможностей ученика.

По результатам исследования современных источников информации можно выделить несколько наиболее популярных, а также часто используемых средств создания интерактивных элементов для обучения игре на музыкальных инструментах. Их можно разделить на три категории, которые различаются по способу взаимодействия с конечным пользователем:

– для создания web интерактивных элементов на web-сайтах;

– для создания интерактивных элементов, работающих в приложениях для мобильных устройств и персональных компьютеров;

– для создания интерактивных элементов, рассчитанных для технологии виртуальной реальности (далее VR) [1].

При создании интерактивных элементов в среде web-разработки используется язык JavaScript. Данный язык позволяет добавлять на web-сайты различные интерактивные элементы, с которыми пользователь может взаимодействовать. Работа с данным языком не требует наличие специальной программы, однако наличие утилиты сильно облегчит работу с JavaScript.

Примером такой утилиты является Visual Studio Code (далее VS code). VS code имеет встроенную поддержку языков JavaScript, TypeScript, Node.js, а также большое количество дополнительно подключаемых языков. Данная утилита обладает следующими возможностями, которые облегчают процесс написания кода: подсветка синтаксиса, сворачивание блоков кода, автоматическое форматирование кода, мульти-строковое редактирование кода (редактирование нескольких строк одновременно, вертикальное выделение), поиск по файлам. поддержка регулярных выражений, встроенная система контроля версий, поддержка git. поддержка других систем контроля версий, используя подключаемые модули (расширения). VS code имеет современный не перегруженный и отзывчивый интерфейс. Вся работа ведется внутри главного окна. Оно разделяется на различные области. Новые окна открываются, как новая область или как всплывающие вспомогательные окна [3, 6].

Перечисленные выше особенности позволяют эффективно работать над созданием интерактивных элементов web страниц и используют язык JavaScript.

При создании интерактивных элементов для приложений используются такие языки как: Java, Kotlin, C++. С целью сделать работу с этими языками более удобными существует множество полезных утилит. Как пример можно выделить Android Studio.

Android Studio это интегрированная среда разработки для работы с платформой Android. Она позволяет работать с вышеперечисленными языками. Также не маловажным преимуществом является встроенный в программу эмулятор, позволяющий проверить корректную работу приложения на устройствах с разными экранами, с различными соотношениями сторон. Среда разработки для приложений Android Studio последней версии стала по-настоящему удобной даже для начинающих разработчиков. В программе реализованы все современные средства для упаковки кода, его маркировки, а наличие функции просмотра приблизительных показателей производительности при запуске приложения на самых популярных устройствах, позволяет разработчику качественно оптимизировать выпускаемый продукт. Также Android Studio позволяет разрабатывать приложения не только для смартфонов/планшетов, а и для персональных компьютеров, приставок

для телевизоров Android TV, устройств Android Wear, мобильных устройств с необычным соотношением сторон экран [4, 5].

При создании интерактивных элементов с использованием технологии VR используются специальные утилиты, которые помогут при создании визуализировать полученный результат. Примером такой утилиты является Unity, которая является межплатформенной средой разработки компьютерных приложений и позволяет создавать приложения, работающие под более чем 20 различными операционными системами, включающими персональные компьютеры, игровые консоли, мобильные устройства, интернет-приложения и другие [2].

Высокая интерактивность VR-приложений заключается в возможности простым перетаскиванием компонентов в сцену выстраивать необходимые объекты и окружение, необходимые разработчику. Также немаловажным фактом для музыкального приложения является наличие усиленного эффекта присутствия в виртуальных средах благодаря встроенной поддержке аудиоклипов с пространственным звучанием, полносферного объемного звука, возможностям настройки ориентации звуковых полей в соответствии с положением слушателя.

В каждом подходе к созданию ресурса с интерактивными элементами имеются как положительные, так и отрицательные стороны. В случае с категорией web интерактивных элементов выделяются следующие положительные стороны:

– общедоступность, которая заключается в необходимости наличия у пользователя персонального компьютера или другого устройства, с возможностью посещения web-страниц;

– простота разработки.

К минусам же можно отнести следующие элементы:

– низкая гибкость разрабатываемых интерактивных элементов;

– сложная адаптация под мобильные платформы.

Разрабатывая приложения для мобильных платформ и персональных компьютеров, разработчик имеет следующие преимущества:

– широкое распространение мобильных платформ и персональных компьютеров;

– широкие возможности для реализации идей;

– доступность в любое время, включая возможность доступа к приложению, при помощи мобильных платформ, из любого места.

Однако данных подход к разработке интерактивных элементов обладает и рядом недостатков:

– необходимость адаптации приложения под различные виды платформ;

– ограниченность создания некоторых решений для небольших экранов устройств.

При выборе инструментов для создания интерактивных элементов необходимо учитывать все выделенные достоинства и недостатки для правильного решения и получения лучшего результата.

В наше время активно развивается технология VR. Она позволяет пользователю погрузится в предлагаемую среду и активно с ней взаимодействовать. В разработке интерактивных элементов в данном направлении также можно отметить как положительные, так и отрицательные моменты:

- Большое разнообразие вариантов использования виртуального пространства;
- Возможность взаимодействия с музыкальными инструментами в виртуальном пространстве.
- Платформа виртуальной реальности только начинает активно развиваться, вследствие чего она не лишена недостатков:
- Большая стоимость данной платформы;
- Сложность в разработке, которая заключается в необходимости привлечения людей из разных областей разработки, таких как: программирование, моделирование объемных объектов, постановщиков сцен, специалистов по работе с пространственным звуком;
- Низкая распространенность данной платформы из-за чего существенно сужается круг потенциальных потребителей.

Наличие такого разнообразия подходов к реализации ресурса с интерактивными элементами позволяет разработчику выбирать платформу и целевую аудиторию, в зависимости от выбранного метода разработки. Для решения проблемы обучения игры на различных инструментах в дистанционной форме необходимо создание отдельного приложения для мобильных платформ и персональных компьютеров. Это объясняется распространенностью данных платформ, а также возможностью взаимодействия с ресурсом без подключения к сети интернет. Создавая интерактивные элементы для web-страниц, разработчик может рассчитывать только на простейшие интерактивные элементы, а при разработке приложений открывается больше возможностей. Доступно больше языков программирования, вследствие чего разнообразие и сложность наполнения создаваемых интерактивных элементов возрастет.

Однако не стоит забывать о возможностях виртуальной реальности, которая в данный момент активно развивается. Технология VR позволяет сделать окружающие элементы готовыми к взаимодействию с пользователем. Это даст возможность создавать элементы, с которыми можно активно взаимодействовать. При должном проектировании все пространство вокруг станет интерактивным, что способствует его превращению в интерфейс для общения с пользователем.

Список используемых источников

1. Приложение для Android. URL: https://skillbox.ru/media/code/kak_sdelat_prilozhenie_dlya_android/ (дата обращения 12.02.2021).
2. Unity URL: https://unity.com/ru (дата обращения 16.02.2021).
3. Visual Studio Code. URL: https://webdesign-master.ru/blog/tools/2018-03-18-visual-studio-code.html (дата обращения 13.02.2021).
4. Android Studio. URL: https://arduinoplus.ru/android-studio/ (дата обращения 11.02.2021).
5. Android Studio IDE от Google. URL: https://wnfx.ru/android-studio-ide-ot-google/#:~:text=Android%20Studio%20%E2%80%94%20%D0%B8%D0%BD%D1%82%D0%B5%D0%B3%D1%80%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D0%B0%D1%8F%20%D1%81%D1%80%D0%B5%D0%B4%D0%B0%20%D1%80%D0%B0%D0%B7%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%BA%D0%B8,%D0%BD%D0%B0%20Windows%2C%20Mac%20%D0%B8%20Linux.&text=IDE%20%D0%BC%D0%BE%D0%B6%D0%BD%D0%BE%20%D0%B7%D0%B0%D0%B3%D1%80%D1%83%D0%B7%D0%B8%D1%82%D1%8C%20%D0%B8%20%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D1%8C%D1%81%D1%8F%20%D0%B1%D0%B5%D1%81%D0%BF%D0%BB%D0%B0%D1%82%D0%BD%D0%BE (дата обращения 12.02.2021).
6. Расширения для VS Code и программирование на JavaScript. URL: https://habr.com/ru/company/ruvds/blog/354960/ (дата обращения 22.03.2021).

УДК 004.021
ГРНТИ 27.41.41

ГЕНЕРАЦИЯ И ПОИСК КРАТЧАЙШЕГО ПУТИ В ДВУМЕРНЫХ ЛАБИРИНТАХ

А. В. Дагаев, Л. А. Коваленко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются алгоритмы генерации и поиска кратчайшего пути в двумерных лабиринтах, а также их характеристики. Целью исследования является определение зависимости времени работы алгоритмов поиска кратчайшего пути от характеристик лабиринтов. Все рассматриваемые характеристики описаны подробным образом. Подобраны такие алгоритмы генерации, результирующие лабиринты которых обладают разными характеристиками, что позволяет определить искомую зависимость. Генерацию лабиринтов осуществляют следующие алгоритмы: «Aldous – Broder», «Recursive Backtracking», «Growing Tree», «Sidewinder», «Rooms» и «Vertical Blocks». Поиск кратчайшего пути осуществляют следующие алгоритмы: «A» с четырьмя эвристиками и «BFS» (поиск в ширину). Особенность применения результата данного исследования заключается в том, что под алгоритм генерации или под конкретные характеристики уже сгенерированного лабиринта можно подобрать наиболее быстрый алгоритм поиска.*

генерация идеальных и неидеальных лабиринтов; поиск кратчайшего пути оптимизация.

Описание лабиринтов

Известно, что лабиринты могут быть организованы по различным классификациям: измерение, гиперпространство, топология, тесселяция, маршрутизация, текстура и фокус [1, 2, 3, 4]. Лабиринт может взять по одной характеристики, в любой комбинации. Сегодня известны различные алгоритмы создания лабиринтов, например алгоритмы: растущего дерева, муравьиные, Уилсона, двоичного дерева и другие [5, 6, 7]. Но в представленных источниках уделяется мало внимания сравнению и оптимизации построения и обхода лабиринтов. В представленной статье показан анализ и сравнение алгоритмов генерации лабиринтов. Итак, лабиринт – это множество пустых и непустых клеток пространства, образующих запутанные пути. Непустые клетки называются стенами, а по пустым клеткам проходит путь.

Далее предполагается, что направлений движения всего 4: влево, вверх, вправо, вниз. Таким образом, путь не следует по диагонали.

Идеальный лабиринт – это лабиринт, в котором одна пустая клетка связана с другой пустой одним единственным путем. Создание идеального лабиринта происходит путем его «выращивания», которое обеспечивает отсутствие циклов и изолированных областей. Такие лабиринты генерируются либо методом добавления стен, либо методом удаления стен. Рассматриваются следующие алгоритмы генерации идеальных лабиринтов: «*Aldous – Broder*», «*Recursive Backtracking*», «*Growing Tree*», «*Sidewinder*».

Неидеальный лабиринт – лабиринт с хотя бы одним циклом или недостижимой областью. Число путей между двумя произвольными пустыми клетками может быть любым. Это также значит, что путь между ними может отсутствовать. Рассматриваются следующие алгоритмы генерации неидеальных лабиринтов: «*Rooms*» и «*Vertical Blocks*» (их реализации не столь важны, сколь их характеристики).

Характеристики рассматриваемых лабиринтов приведены в таблице.

ТАБЛИЦА. Алгоритмы генерации лабиринтов

Алгоритм	% тупиков	Тип	Фокус	Отсутствует смещенность	Однородность
«Aldous – Broder» *Решение: 13 %*	14	Дерево	±	Да	Да

Алгоритм	% тупиков	Тип	Фокус	Отсутствует смещенность	Однородность
«Recursive Backtracking» *Решение: 22 %*	13	Дерево	–	Да	Никогда
«Growing Tree» *Решение: 3/20/4 %*	2/13/23	Дерево	±	Да	Нет
«Sidewinder» *Решение: 4 %*	24	Множество	±	Нет	Никогда
«Rooms» *Решение: 2 %*	39	—	±	Да	Никогда
«Vertical Blocks» *Решение: 1 %*	≈0	—	±	Нет	Никогда

Решение. Это отношение количества клеток решения лабиринта к числу всех пустых клеток. Предполагается, что размер лабиринта 101×101, а среднее значение выведено на основе 100 тестов. Кроме того, начало и конец каждого решения находится в противоположных краях лабиринта (слева и справа, сверху и снизу). Этот параметр является показателем «извилистости» пути решения. Максимальную извилистость имеют одномаршрутные лабиринты, потому что решение проходит по всему лабиринту. Минимально возможную извилистость имеет лабиринт, у которого решение идет строго в одном направлении от начала к концу. Для алгоритма «Growing Tree» приведены значения при способах выбора «первая добавленная клетка» (3 %), «последняя добавленная клетка» (20 %) и «любая из добавленных клеток» (4 %).

Тупики. Это отношение количества пустых клеток, которые являются тупиками (то есть около них ровно три стены и одна пустая клетка), к числу всех пустых клеток. Для алгоритма «Growing Tree» представлены значения при способах выбора «первая добавленная клетка» (2 %), «последняя добавленная клетка» (13 %) и «любая из добавленных клеток» (23 %). Максимально возможный процент тупиков в идеальном лабиринте составляет 66 % – это маршрут с тупиками единичной длины по обеим сторонам от него.

Тип. Существует два типа алгоритмов создания идеальных лабиринтов:

– Алгоритм на основе дерева: выращивает лабиринт подобно дереву, всегда добавляя к тому, что уже есть, и на каждом этапе имея правильный идеальный лабиринт.

– Алгоритм на основе множеств: строит так, как считает нужным, отслеживая все части лабиринта, чтобы на момент завершения соединить их и получить идеальный лабиринт.

Алгоритмы создания неидеальных лабиринтов могут быть реализованы любым образом (дерево и/или множества необязательны).

Фокус. «+» означает, что реализовать алгоритм можно только через добавление стен (изначально поле без стен), «–» означает, что только через удаление стен (изначально поле со всеми стенами), «±» допускает оба варианта. «Recursive Backtracking» нельзя реализовать через добавление стен, так как в этом случае он склонен создавать путь решения, который следует вдоль края лабиринта, а вся внутренняя часть соединена с границей единственным проходом.

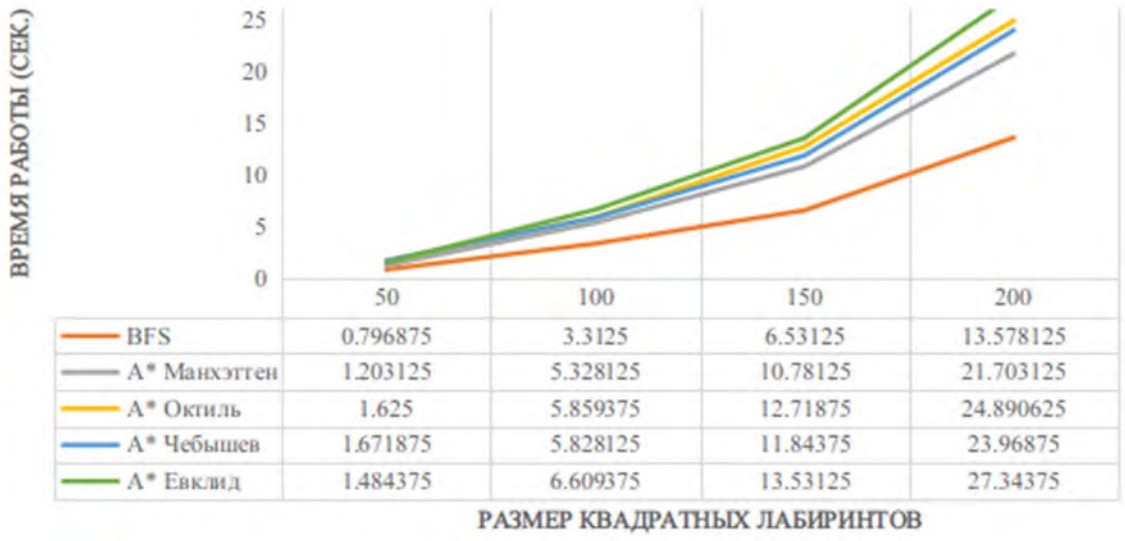
Отсутствие смещенности. Смещенность присутствует, если некоторые или все проходы склонны больше идти в одном направлении, чем в другом. Алгоритм «Sidewinder» смещен, в нем легко перемещаться снизу вверх и сложно сверху вниз.

Однородность. Алгоритм генерации однороден, если все возможные лабиринты генерирует с равной вероятностью. «Да» означает, что алгоритм полностью однороден. «Нет» означает, что алгоритм потенциально может генерировать все возможные лабиринты, но не с равной вероятностью. «Никогда» означает, что существуют лабиринты, которые алгоритм никогда не сможет сгенерировать. Причем только алгоритмы с полным отсутствием смещенности могут быть полностью однородными.

Алгоритмы поиска. Тестирование и результаты

Для разработки алгоритмов был использован язык программирования Python 3.7.6, разработка велась под операционной системой Microsoft Windows 8.1. Алгоритмы поиска были проверены на поиск именно кратчайшего пути по длине и ошибок обнаружено не было. Алгоритм «Growing Tree» при тестировании использовал только правило выбора «последняя добавленная клетка» (решение сложное и тупиков много).

На рис. 1 представлены результаты тестирования алгоритмов поиска кратчайших путей в идеальных лабиринтах.

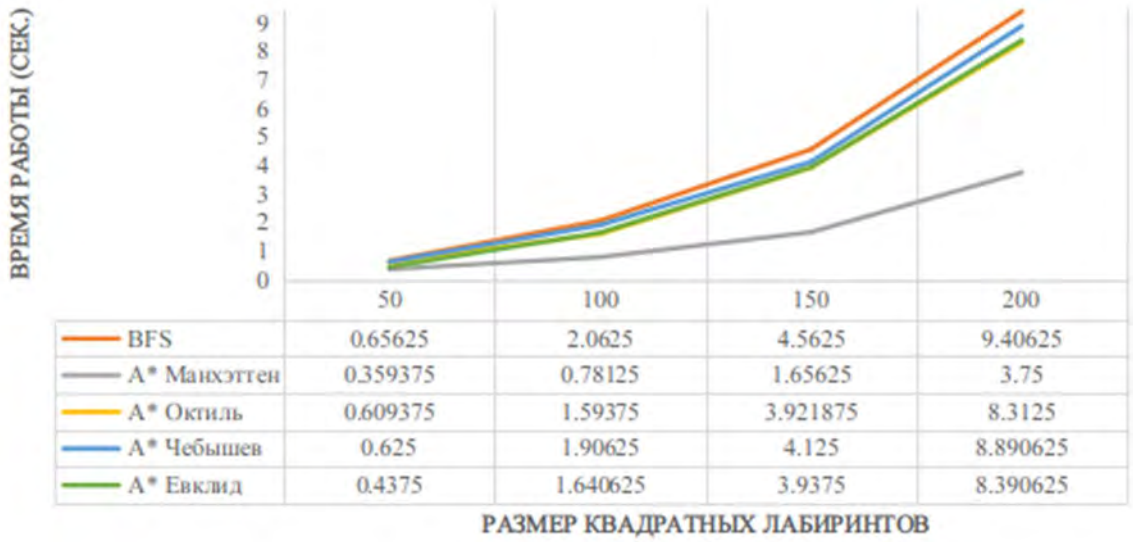


	50	100	150	200
BFS	0.796875	3.3125	6.53125	13.578125
A* Манхэттен	1.203125	5.328125	10.78125	21.703125
A* Октиль	1.625	5.859375	12.71875	24.890625
A* Чебышев	1.671875	5.828125	11.84375	23.96875
A* Евклид	1.484375	6.609375	13.53125	27.34375

Рис. 1. Время работы алгоритмов поиска кратчайших путей в идеальных лабиринтах. Количество тестов: 100

Как можно заметить, алгоритм «BFS» справляется с задачей быстрее всех остальных. Это связано с тем, что решение в идеальном лабиринте извилистое, «BFS» ищет во всех направлениях, а эвристики «A*» ориентируются преимущественно на одно направление движения, поэтому предсказание не всегда верно, из-за чего алгоритму «A*» приходится возвращаться и выбирать другие направления.

На рис. 2 представлены результаты тестирования алгоритмов поиска кратчайших путей в неидеальных лабиринтах.

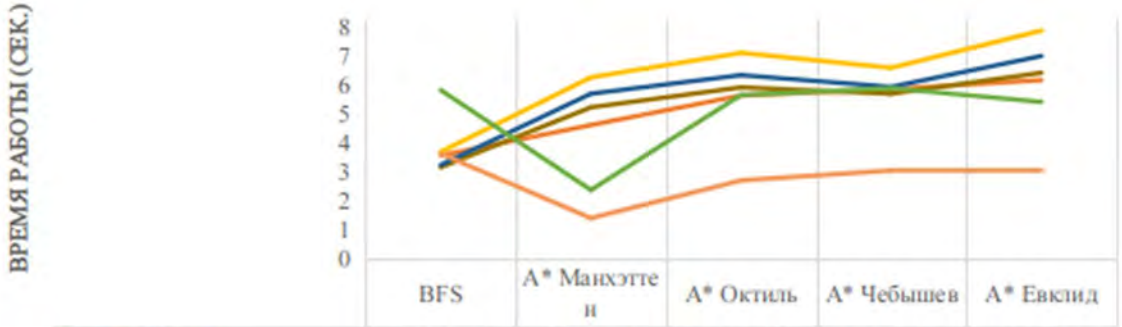


	50	100	150	200
BFS	0.65625	2.0625	4.5625	9.40625
A* Манхэттен	0.359375	0.78125	1.65625	3.75
A* Октиль	0.609375	1.59375	3.921875	8.3125
A* Чебышев	0.625	1.90625	4.125	8.890625
A* Евклид	0.4375	1.640625	3.9375	8.390625

Рис. 2. Время работы алгоритмов поиска кратчайших путей в неидеальных лабиринтах. Количество тестов: 100.

Из рис. 2 видно, что «A*» с эвристикой расстояния Манхэттена работает быстрее остальных. Это связано с тем, что координатные шаги алгоритма определяются четырьмя направлениями и сама эвристика измеряет расстояние между точками четырьмя направлениями, благодаря чему предсказание происходит более точно, чем при других эвристиках. Алгоритм «BFS» работает медленно, так как осуществляет поиск во всех направлениях независимо от расстояний между клетками.

На рис. 3 представлены более подробные результаты тестирования алгоритмов поиска кратчайших путей.



	BFS	A* Манхэттен	A* Октиль	A* Чебышев	A* Евклид
Sidewinder	3.546875	4.59375	5.609375	5.828125	6.140625
Recursive Backtracking	3.671875	6.234375	7.078125	6.5625	7.84375
Aldous-Broder	3.140625	5.203125	5.890625	5.671875	6.390625
Growing Tree	3.21875	5.671875	6.3125	5.90625	6.96785
Rooms	3.609375	1.390625	2.6875	3.03125	3
Vertical Blocks	5.796875	2.359375	5.625	5.859375	5.390625

Рис. 3. Время работы алгоритмов поиска кратчайших путей в лабиринтах размера 200×200. Количество тестов: 100

Вывод

Для алгоритмов генерации идеальных лабиринтов и им подобных структур подходит больше алгоритм поиска «BFS», а для алгоритмов генерации неидеальных лабиринтов (или структур с большим количеством свободных клеток) подходит больше «A*» с эвристикой расстояния Манхэттена (или других эвристик в случае иных определений координатных шагов). Данные исследования также могут быть полезны при анализе сетевой маршрутизации, поиска путей в лабиринтах и разнородных сетевых структурах.

Список используемых источников

1. Think Labyrinth: Maze algorithms. URL: https://www.astrolog.org/labyrnth/algrithm.htm.

2. Implementation of A*. URL: https://www.redblobgames.com/pathfinding/a-star/implementation.html.

3. Aldous – Broder algorithm. URL: https://weblog.jamisbuck.org/2011/1/17/maze-generation-aldous-broder-algorithm.html.

4. Backtracking algorithm. URL: https://weblog.jamisbuck.org/2010/12/27/maze-generation-recursive-backtracking.

5. Growing Tree algorithm. URL: https://weblog.jamisbuck.org/2011/1/27/maze-generation-growing-tree-algorithm.

6. Sidewinder algorithm. URL: https://weblog.jamisbuck.org/2011/2/3/maze-generation-sidewinder-algorithm.html.

7. Классические алгоритмы генерации лабиринтов. Часть 1: вступление. URL: https://habr.com/post/320140/; 2. Классические алгоритмы генерации лабиринтов. Часть 2: погружение в случайность. URL: https://habr.com/post/321210/

УДК 004.032
ГРНТИ 28.23.37

СРАВНИТЕЛЬНЫЙ АНАЛИЗ РАЗЛИЧНЫХ МОДЕЛЕЙ НЕЙРОННЫХ СЕТЕЙ И ФУНКЦИЙ ОШИБОК В ЗАДАЧЕ СЕГМЕНТАЦИИ КОЖНЫХ ЗАБОЛЕВАНИЙ

А. В. Дагаев, М. Э. Чмелёв

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В последнее время задача сегментации в медицине становится все более актуальной. В данной статье рассмотрена задача сегментации кожаных заболеваний с использованием различных моделей машинного обучения. В статье проведён сравнительный анализ результата обучения моделей свёрточных нейронный сетей с применением различных функций ошибок. Приведены результаты работы моделей на валидационной выборке.

SegNet, U-net, Dilated U-net, свёрточная нейронная сеть, Focal loss, Tversky loss, Dice loss, сегментация.

В качестве исходных данных был использован *PH^2 dataset* [1], содержащий 200 изображений меланом размером 765×573 пикселей. Каждое изображение было приведено к размеру 256×256 (рис. 1). Весь датасет был разбит на три части для обучения, валидации и тестирования размером соответственно 100:50:50. В качестве моделей для сегментации были использованы: *SegNet* [2], *U-net* [3], *Dilated U-net* [4].

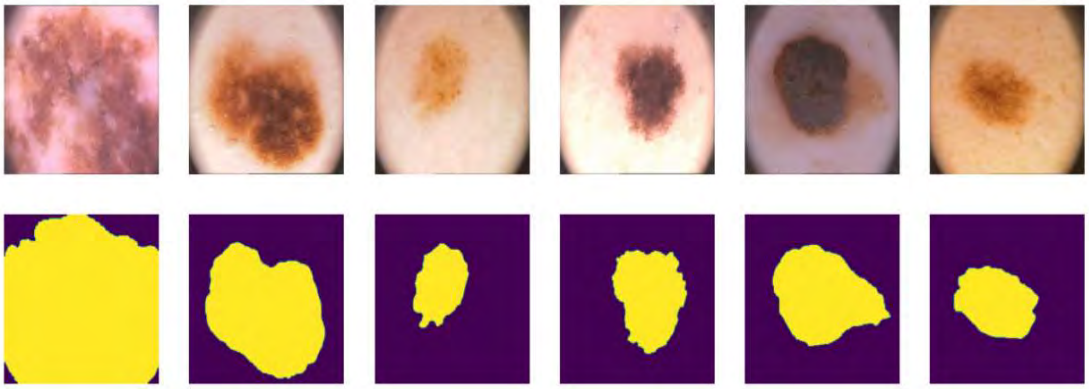


Рис. 1. Пример исходных данных

В качестве модели для тестирования различных функций ошибок был использована *SegNet*. *SegNet* считается предшественником остальных моделей и была выбрана исходя из того, что другие модели выдадут результат, по крайней мере, не хуже данного. Результаты модели сравнивались по метрике *IoU* [5] (1), посчитанной на тестовой части датасета. Каждая из моделей училась на тренировочной части 40 эпох, используя оптимизатор *AdamW* [6] с параметрами: *lr* = 0.0001, *betas* = (0.9, 0.999), *eps* = 1e-08, *weight_decay* = 0.01.

$$IoU = \frac{target \cap prediction}{target \cup prediction}. \quad (1)$$

Бинарная кросс-энтропия (2) является популярной функцией ошибки и подходит для нашей задачи. Проблемой оказалось то, что данная функция ошибки страдает от численной нестабильности.

$$BCE(y, \hat{y}) = -\sum_i [y_i log\sigma(\hat{y}_i) + (1 - y_i) \log\big(1 - \sigma(\hat{y}_i)\big)] . \quad (2)$$

Используя упрощение Тарая данная функция была приведена к эквивалентной (3).

$$BCE(y, \hat{y}) = \hat{y} - y\hat{y} + \log(1 + \exp(-\hat{y})). \quad (3)$$

Результат обучения модели с использованием данной функции ошибки представлены на (рис. 2).

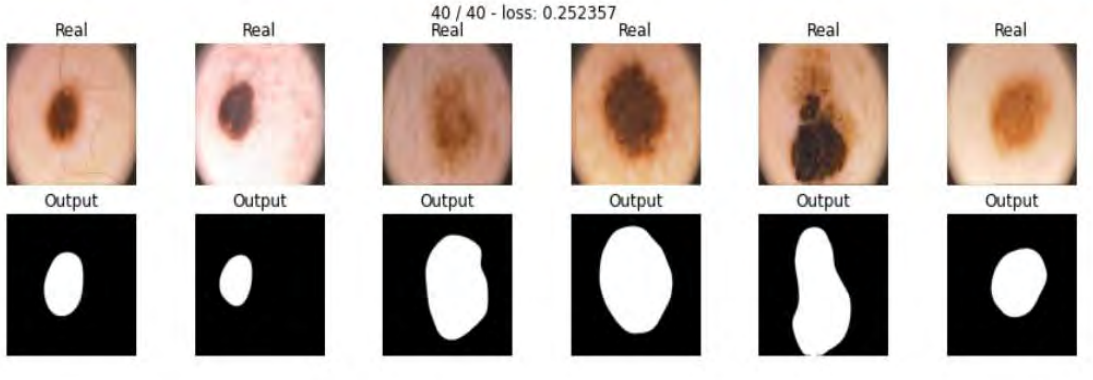


Рис. 2. Результат обучения модели с использованием *Binary Cross-Entropy*

Следующей функцией ошибки был выбран *Dice Loss* (4):

$$DiceLoss(y, \hat{y}) = 1 - \sum_i [\frac{2y_i\hat{y}_i}{{y_i}^2 + {\hat{y}_i}^2}]. \quad (4)$$

Результат обучения модели с использованием данной функции ошибки представлены на (рис. 3).

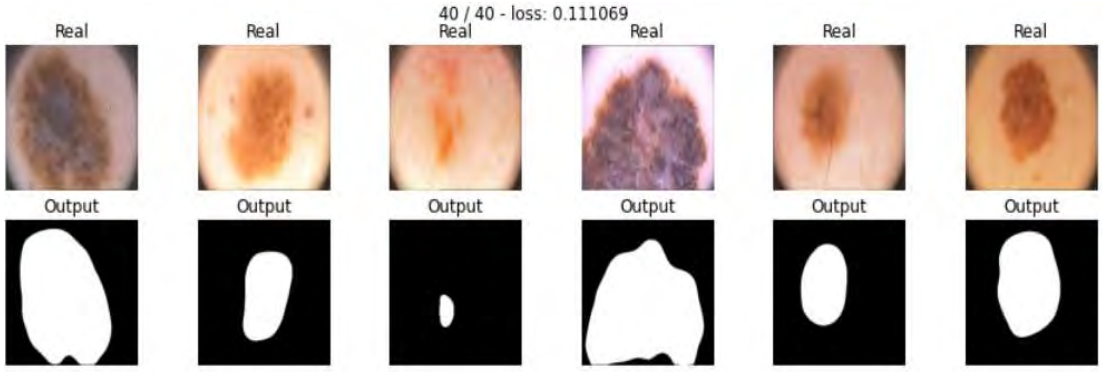


Рис. 3. Результат обучения модели с использованием *Dice Loss*

Одной из возможных проблем в задачи сегментации медицинских снимков является неравномерность распределения классов. Исправить данный дисбаланс может помочь *Focal loss* [7] (5), благодаря взвешиванию вероятности предсказания класса пикселя.

$$Focal(y, \hat{y}) = -\sum_i [\big(1 - \sigma(\hat{y}_i)\big)^{\gamma} y_i log\sigma(\hat{y}_i) + (1 - y_i)\log\big(1 - \sigma(\hat{y}_i)\big)]. \quad (5)$$

В ходе эксперимента переменная γ была зафиксирована на значении 2. Результат обучения модели с использованием данной функции ошибки представлены на (рис. 4).

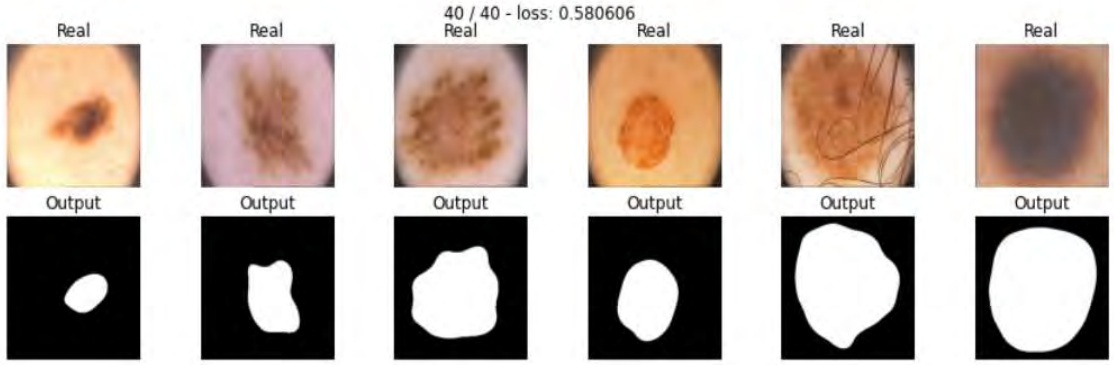


Рис. 4. Результат обучения модели с использованием *Focal Loss*

Ещё одной функцией ошибок, позволяющей минимизировать влияние дисбаланса классов, была выбрана *Tversky Loss* [8] (6). В ходе эксперимента переменная α была зафиксирована на значении 0.3:

$$TverskyLoss\ (y, \hat{y}) = \ 1 - \sum \frac{y\hat{y}}{y\hat{y} + \alpha\ \ (1-\hat{y}) + (1-\alpha)(1-y)\hat{y}}\ . \qquad (6)$$

Результат обучения модели с использованием данной функции ошибки представлены на (рис. 5).

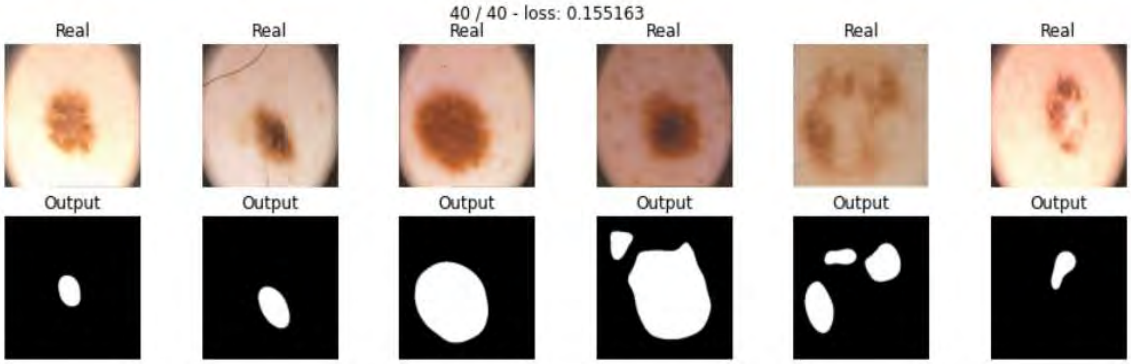


Рис. 5. Результат обучения модели с использованием *Tversky Loss*

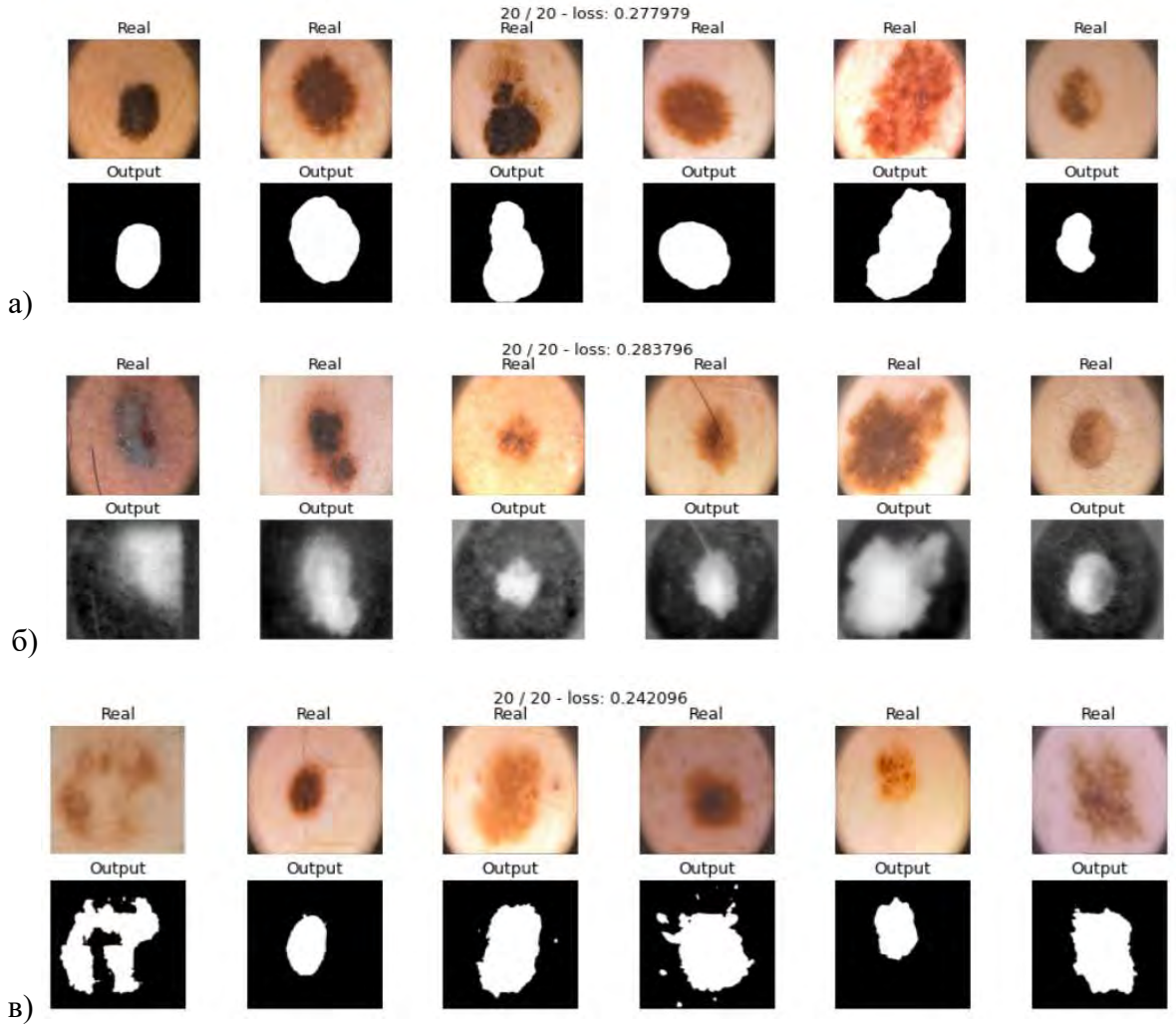
В ходе эксперимента удалось добиться лучшего результата, используя функцию ошибки *BCE Loss*. Это говорит о том, что дисбаланса класса не наблюдается либо же он находится в допустимых значениях и на процесс обучения негативно не сказывается. Результаты всех экспериментов приведены в таблице 1.

ТАБЛИЦА 1. Значения метрики в зависимости от используемой функции ошибок

Используемая функция ошибки	Значение метрики *IoU*
BCE Loss	**0.505**
Dice Loss	0.501

Используемая функция ошибки	Значение метрики *IoU*
Focal Loss	0.417
Tversky Loss	0.4

После того как мы определились с функцией ошибок, стоит перейти к более сложным моделям. *U-net* отличается от *SegNet* тем, что в ней происходит перенос скрытых состояний нейронов между слоями сети. В качестве восстановления изображения из скрытого состояния используют несколько подходов. Проверим наиболее популярные их них, а именно: слои *Upsample*, *Conv-Transpose*. Проверим так же подход, основанный на использовании расширенной свертки. Опытным путём было выявлено, что для обучений моделей *U-net* требуется в два раза меньше эпох чтоб выйти на плато ошибки. Результаты обучения моделей представлены на (рис. 6).



а)

б)

в)

Рис. 6. Результаты обучения моделей:
а) результат классической *U-net, Upsample* слои,
б) результат *U-net, Conv-Transpose* слои,
в) результат *U-net. Conv-Transpose + Dilated* слои

В ходе эксперимента лучшего результата добилась *U-net* с *Conv-Transpose* и *Dilated* слоями. Моделе удалось получить существенный отрыв, что является хорошим результатом. Результаты всех экспериментов приведены в таблице 2.

ТАБЛИЦА 2. Значения метрики в зависимости от используемой модели

Используемая функция ошибки	Значение метрики *IoU*
U-net	0.452
U-net + Transposed	0.43
U-net + Transposed + Dilated	**0.642**
SegNet best score	0.505

Выводы

Современные модели машинного обучения уже сейчас справляются с данной задачей. Использование алгоритмов сегментации изображения может значительно ускорить предварительную обработку изображения и помочь медикам в работе с кожаными заболеваниями. В качестве модели следует использовать *U-net* с *Dilated* слоями свертки. В качестве функции ошибок следует использовать *cross-entropy loss.*

Список используемых источников

1. Teresa Mendonca, Pedro M. Ferreira, Jorge S. Marques, Andre R. S. Marcal Jorge Rozeira. PH2-A dermoscopic image database for research and benchmarking // Conference proceedings: Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Conference 2013:5437-5440, 2013.

2. Badrinarayanan, Vijay; Kendall, Alex; Cipolla, Roberto. SegNet: A Deep Convolutional Encoder-Decoder Architecture for Image Segmentation // arXiv preprint arXiv: 1511.00561, 2016.

3. Ronneberger, Olaf; Fischer, Philipp; Brox, Thomas. U-Net: Convolutional Networks for Biomedical Image Segmentation // arXiv preprint arXiv: 1505.04597, 2016.

4. Vesal, Sulaiman; Ravikumar, Nishant; Maier, Andreas. A 2D dilated residual U-Net for multi-organ segmentation in thoracic CT // arXiv preprint arXiv: 1905.07710, 2019.

5. Zheng, Zhaohui; Wang, Ping; Liu, Wei; Li, Jinze; Ye, Rongguang; Ren, Dongwei. Distance-IoU Loss: Faster and Better Learning for Bounding Box Regression // arXiv preprint arXiv: 1911.08287, 2019.

6. Loshchilov, Ilya; Hutter, Frank. Decoupled Weight Decay Regularization // arXiv preprint arXiv: 1711.05101, 2019

7. Tsung-Yi Lin Priya Goyal Ross Girshick Kaiming He Piotr Dollar. Focal Loss for Dense Object Detection // arXiv preprint arXiv: 1708.02002v2, 2018

8. Seyed Sadegh Mohseni Salehi, Deniz Erdogmus, Ali Gholipour. Tversky loss function for image segmentation using 3D fully convolutional deep networks 2017 // arXiv preprint arXiv: 1706.05721, 2017

УДК 004.942
ГРНТИ 49.33.35

ПРОБЛЕМЫ РЕАЛИЗАЦИИ СОВРЕМЕННЫХ СИСТЕМ ОБНАРУЖЕНИЯ КИБЕРНЕТИЧЕСКИХ АТАК

А. И. Еременко, А. В. Кокорев, К. Ф. Слесарчик, С. Н. Шведов

Академия Федеральной службы охраны Российской Федерации

В статье рассматриваются концептуальные трудности реализации систем обнаружения кибернетических атак на современной электронной базе при использовании статистических и эвристических методов обнаружения деструктивных информационных кибернетических воздействий. Предложены направления преодоления указанных в статье проблем, позволяющие привести в соответствие сложившийся дисбаланс характеристик инфокоммуникационных сетей и возможностей систем обнаружения кибернетических атак.

система обнаружения кибернетических атак, многовекторная DDoS-атака, искусственная нейронная сеть, инфокоммуникационная сеть, деструктивное информационное кибернетическое воздействие.

Анализ ТТХ программно-аппаратных, программных комплексов и средств (ПАК, ПК, ПС) обнаружения деструктивных информационных кибернетических воздействий (ДИКВ) показывает (табл. 1) [1], что относительно низкая производительность отечественных систем обнаружения вторжений (до 8 Гб/с) является следствием не оптимальности выбора структурных параметров ПАК и ПК. Возникшая проблема объясняется различными закономерностями эволюционного развития информационной и технологической составляющих технологического уклада. Информационная составляющая развивается по экспоненциальному закону, а технологическая по линейному с эпизодическими скачками.

ТАБЛИЦА 1. Характеристики программных и программно-аппаратных комплексов обнаружения вторжений отечественного производства

Наименование комплекса	Технология	Производительность МЭ, Гб/с	Производительность СОВ, Гб/с	Тип
Numa Edge	SEIM-платформа	до 38,6	до 4,2 Гб/с	ПАК
«Форпост»	SEIM-платформа	-	до 7	ПАК
«Рубикон», «Рубикон-К»	SEIM-платформа	0,6-9	0,4- 3	ПАК

Наименование комплекса	Технология	Производительность МЭ, Гб/с	Производительность СОВ, Гб/с	Тип
«Универсальный шлюз безопасности «UserGate UTM»	-	до 60	до 8	ПАК
«Форпост 3.0»	SEIM-платформа	-	до 7	ПК
«С-Терра СОВ»	SEIM-платформа	-	до 6	ПК
ПК «Аргус»	SEIM-платформа	-	Зависит от аппаратной платформы	ПК
ПС СОВ «Кречет»	SEIM-платформа	-	до 7,5	ПС

Существующие подходы к выбору методов обнаружения кибернетических вторжений не позволяют достичь приемлемых значений производительности систем обнаружения вторжений (СОВ), что подтверждают результаты анализа производительности устройств хранения информации (УХИ) и ОЗУ (рис. 1).

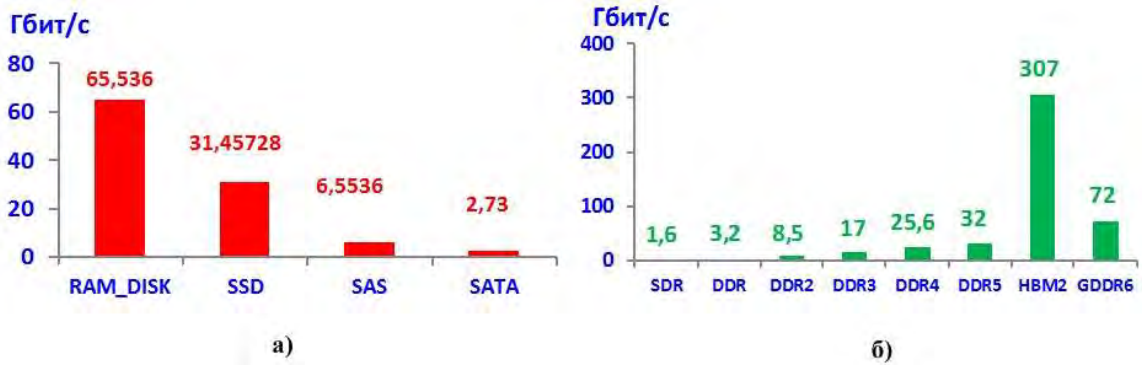


Рис. 1. Технические характеристики современных устройств хранения информации (а) и оперативно-запоминающих устройств (б)

Совместный анализ статистики структуры ДИКВ (рис. 2.) [2, 3, 4], и ТТХ УХИ и СОВ показал не соответствие используемых методов обнаружения кибер-атак существующим возможностям технологической базы и как следствие уровню, поставленных объективной реальностью, задач.

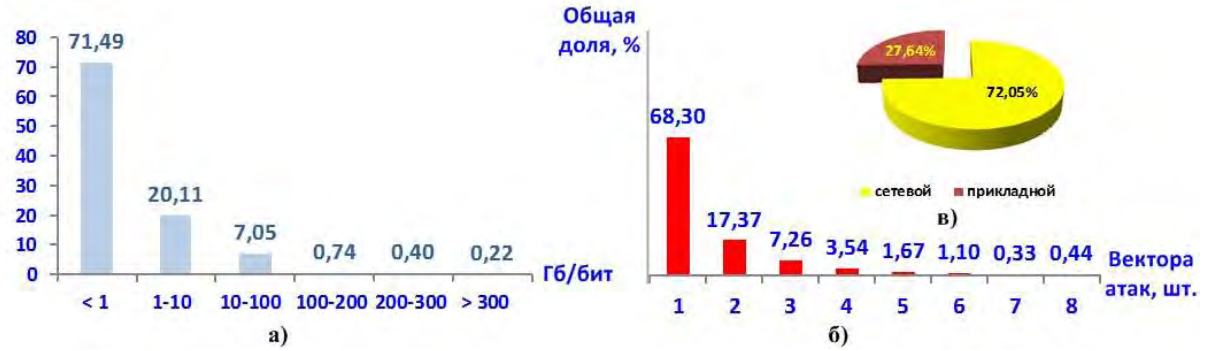


Рис. 2. Средняя мощность (а) и многовекторность (б) DDoS-атак, а также соотношение атак на протоколы сетевого и прикладного уровней за 2018–2020 года

Преимущества и недостатки существующих методов обнаружения ДИКВ показаны в таблице 1. Решение задачи обнаружения многовекторной DDoS-атаки (1) статистическими, сигнатурными и «Data Mining» методами не позволяют реализовывать СОВ с требуемой на существующий момент производительностью.

$$\left(\forall\{a_i\} \supset A\right)\exists arg\, max_{m_i \in M}\, grad\left(m_j[a_i]\right), i = 1\ldots n,\ j = 1\ldots k$$

где $A\{a_i\}$ – множество векторов характеристик типов атак;

m_j – вектор метрик соответствующих i типу атаки;

$M\{m_j\}$ – множество векторов метрик соответствующих атаке.

ТАБЛИЦА 2. Методы обнаружения DDoS-атак

№ п/п	Метод	Достоинства	Недостатки
1.	Статистический (методы Хертса, контрольных карт EWMA, коммуника-ционной матрицы и др.) [5, 6, 7, 8, 9]	Адаптация к поведению субъекта, не требуется знание о возможных атаках и используемых уязвимостях	1. Возможность манипуляции эталонными профилями параметров трафика 2. Объективная трудность определения граничных (пороговых) значений отслеживаемых характеристик.
2.	Использование экспертных систем (сигнатурный метод) [10]	Отсутствие ложных тревог	Необходимость постоянного обновления сигнатур (актуализация).
3.	Использование методов на основе мягких решений (нейросетевые анализаторы) [11, 12]	Способность идентифицировать элементы, которые не похожи на те, что наблюдались ранее.	Точность обнаружения атак зависит от качества обучения нейросети.

№ п/п	Метод	Достоинства	Недостатки
4.	Использование методов Data Mining и машинного обучения [13, 14]	Малое время обнаружения события атаки	1. Недостаточно апробирован на практике. 2. Требует достаточно больших вычислительных мощностей.

Одним из направлений преодоления существующей проблемы производительности СОВ является реализация методов на основе мягких решений на базе ПЛИС, что позволит оставлять неизменной вычислительную ёмкость при разрастании архитектуры ИНС. Пример реализации анализатора многовекторной DDoS-атаки типа LowDDoS-TCP$_{flood}$-ICMP$_{flood_app}$ показан на рис. 3 [12].

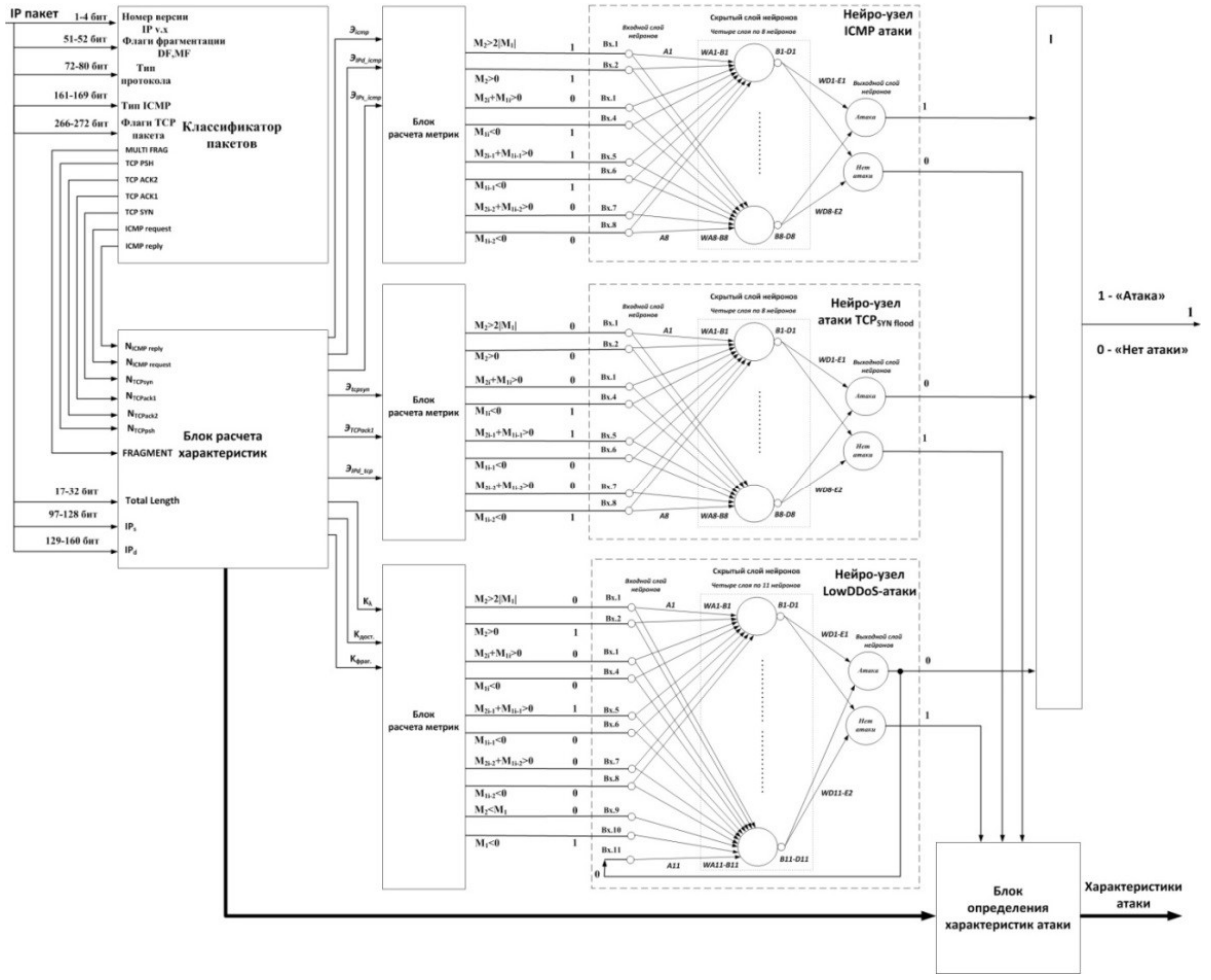


Рис. 3. Схема устройства обнаружения многовекторной атаки вида LowDDoS-TCP$_{flood}$-ICMP$_{flood_app}$

Вторым направлением преодоления дисбаланса между характеристиками инфокоммуникационных сетей и возможностями СОКА является пе-

реход от параметрических принципов фильтрации трафика к характеристическим, что позволит [15]: классифицировать принадлежность трафика к любому ПО без трудоемкого анализа параметров заголовков IP-пакетов с целью определения последовательности пакетов в сессиях и решать задачи демаскирования протоколов при использовании технологий VPN, PGP и им подобных.

Список используемых источников

1. Государственный реестр сертифицированных средств защиты информации. URL: https://fstec.ru/ (дата обращения 15.11.2020).

2. Threat Report Distributed Denial of Service (DDoS) Q1-Q4 2018-2019, Q1-Q2 2020. URL: https://www.nexusguard.com/ (дата обращения 15.01.2021).

3. Threat Report Distributed Denial of Service (DDoS) Q1-Q4 2018-2019, Q1 2020. URL: https://www.nexusguard.com/ (дата обращения 15.01.2021).

4. HI TECH CRIME TRENDS 2019/2020. URL: https://www.group-ib.com/ (дата обращения 15.06.2020).

5. Щелухин О. И., Антонян А. А. Анализ изменений фрактальных свойств телекоммуникационного трафика вызванных аномальными вторжениями // T-COMM: Телекоммуникации и транспорт. 2014. Т. 8, № 6. С. 61–64.

6. Частикова В. А., Власов К. А., Картамышев Д. А. Обнаружение DDOS-атак на основе нейроных сетей с применением метода роя частиц в качестве алгоритма обучения // Фундаментальные исследования. 2014. № 8-4. С. 829–832.

7. Peng, T.; Leckie, C.; Kotagiri, R. Proactively detecting DDoS attack using source IP address monitoring // The 3rd Int. IFIP-TC6 Networking Conf., in: Lecture Notes in Computer Science, vol. 3042, 2004. Pp. 771–782.

8. Feinstein, L.; Schnackenberg, D.; Balupari, R.; Kindred, D. Statistical approaches to DDoS attack detection and response // DARPA Information Survivability Conf. and Exposition, 2003. Pp. 303–314.

9. Семенов Н. А., Телков А. Ю. Применение статистических методов обнаружения DoS атак в локальной сети // Вестник ВГУ: Системный анализ и информационные технологии. 2012. № 1. С. 82–87.

10. Борисов В. И., Шабуров А. С. О применении сигнатурных методов анализа информации в SIEM-системах // Вестник УРФО. Безопасность в информационной сфере. 2015. № 3 (17). С. 23–27.

11. Слесарчик К.Ф. Обнаружение многовекторных DDoS-атак сетевого и прикладного уровней // Техника радиосвязи. 2019. № 4 (43). С. 56–69. doi 10.33286/2075-8693-2019-43-56-69.

12. Попов А. С. Выявление закономерностей DDOS трафика методами Data mining // В мире научных открытий. 2013. № 10 (46). С. 56–67.

13. Браницкий А. А., Котенко И. В. Анализ и классификация обнаружения сетевых атак // Труды СПИИРАН. 2016. Вып. 2 (45). С. 204–244.

14. Левоневский Д. К., Пичугин Ю. А., Фаткиева Р. Р. Оценка спектральных характеристик трафика в задаче обнаружения компьютерных атак различного типа [Электронный ресурс] // Труды СПИИРАН. 2013. Вып. 7 (30). С. 56–64. URL: https://www.proceedings.spiiras.nw.ru/ (дата обращения: 15.01.2021).

УДК 004.7:004.422.8
ГРНТИ 20.01.07

ВЫЧИСЛИТЕЛЬНЫЙ ИНТЕЛЛЕКТ МОНИТОРИНГА ИНФОРМАЦИОННОЙ ЗАЩИЩЕННОСТИ РАСПРЕДЕЛЕННЫХ СИСТЕМ УЧЕТА

А. О. Жаранова, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Выделены ключевые направления развития вычислительного интеллекта с позиций современных подходов к созданию систем искусственного интеллекта. Рассмотрены приемы введения вычислительного интеллекта в мониторинг информационной защищенности распределенных систем учета. Описаны математические особенности комплексирования средств защиты информации при обеспечении информационной защищенности распределенных систем учета. Раскрыты приемы формирования вычислительного интеллекта мониторинга информационной защищенности распределенных систем учета при оперативном обнаружении появляющихся угроз.

вычислительный интеллект, информационная безопасность, комплексные системы защиты информации, мониторинг, распределенные системы.

Вычислительный интеллект обеспечивает формирование гибкого профиля при принятии решений в части защиты информации в условиях использования распределенных систем и влияния динамической среды. Методы вычислительного интеллекта, как правило, включают в себя нечеткую логику, эволюционные вычисления, системы интеллектуальных агентов, нейронные сети, клеточные автоматы, искусственные иммунные системы, а также другие аналогичные вычислительные модели и могут находить свое отражение в различных отраслях деятельности. Интеграция таких методов позволяет создавать эффективные и надежные модули поддержки принятия решений, формируя оптимальные модели обеспечения информационной безопасности. Вычислительный интеллект применяется в системах извлечения новых знаний из распределенных баз данных, где необходимо принятие решение на основе оценки параметров при многомерном статистическом анализе [1].

С развитием цифровых платформ и технологий, характеризующихся разнообразием архитектурных решений, возрастает востребованность распределенных систем учета и необходимость сложных распределенных операций и вычислений в глобальной сети Интернет, в связи с чем актуализируется вопрос формирования систем мониторинга информационной

защищенности. Для защиты распределенной информационной инфраструктуры необходимо формирование гибких, адаптируемых и надежных агентов обеспечения безопасности, которые могут принимать интеллектуальные решения в режиме реального времени при обнаружении широкого спектра сетевых угроз и атак. Вычислительные интеллектуальные методы все чаще применяются для усиления мер информационной безопасности и становятся основой для формирования комплексных систем защиты информации.

В методологическом аспекте выделяются задачи обеспечения информационной безопасности, которые относятся к классу раннего обнаружения проявляющихся угроз.

Для комплексных систем защиты информации выделяются такие приемы комплексирования, которые предусматривают обеспечение раннего обнаружения угроз информационной безопасности. Как правило такие приемы реализуются согласно логической функции ИЛИ и учитывают фактор распределенности, который характеризуется по стохастическому принципу с учетом отображения плотностей распределения вероятностей времен передачи информации между базовыми компонентами комплексной системы защиты информации [2, 3].

Помимо этого, необходимо учитывать неблагоприятные факторы, связанные с динамикой окружающей среды и появляющимися препятствиями при выполнении задач защиты информации.

Проведем анализ качества функционирования комплексной системы защиты информации с узлом соединения параллельных подсистем на базе функции синхронизации первого уровня «V» и узлом соединения параллельных подпроцессов защиты информации подсистем на базе функции синхронизации второго уровня «V», В процессе анализа преобразуем параллельные подпроцессы, а также полученные последовательности после преобразования для получения плотности распределения времени принятия решения каждой из подсистем защиты информации.

Преобразование параллельных подпроцессов защиты информации подсистемы на базе функции синхронизации «V» осуществляется следующим образом:

$$f_{m,i}\left(k_{m,1,2,\ldots,I}\right)=\prod_{m,i=1}^{m,I}\left(1-\sum_{i=1}^{k_{m,1,2,\ldots,I}-1}f_{m,i}\left(k_{m,i}\right)\right)-\prod_{m,i=1}^{m,I}\left(1-\sum_{k_{m,i}=1}^{k_{m,1,2,\ldots,I}}f_{m,i}\left(k_{m,i}\right)\right),$$

$$k_{m,1,2,\ldots,I}=\min\left(\min k_{m,1},\min k_{m,2},\ldots,\min k_{m,i},\ldots,\min k_{m,I}\right),\ldots,\min\left(\max k_{m,1},\max k_{m,2},\ldots,\max k_{m,i},\ldots,\max k_{m,I}\right),$$

где $m=1,2,\ldots,M$ – порядковый номер подсистемы,

$i=1,2,\ldots,N$ – номер подпроцесса защиты информации подсистемы.

После введения следующих обозначений:

$$f_{m,\vee}\left(k_{M,\vee}\right)=f_{m,I}\left(k_{m,1,2,\ldots,I}\right),$$

$$k_{M,\vee}=k_{m,1,2,\ldots,I}.$$

процесс преобразования полученной последовательности из действий по обеспечению защиты информации $f_{m,0}\left(k_{m,0}\right)$, $f_{m,\vee}\left(k_{m,\vee}\right)$ и $f_{m,mN+1}\left(k_{m,mN+1}\right)$ выполняется в 2 этапа.

Первый этап осуществляется путем преобразования последовательности из действий, описываемых плотностями $f_{m,0}\left(k_{m,0}\right)$ и $f_{m,\vee}\left(k_{m,\vee}\right)$:

$$f_{(m,0),(m,\vee)}\left(k_{(m,0),(m,\vee)}\right)=\sum_{\min k_{m,0}}^{\max k_{m,0}} f\left(k_{m,0}\right) f_{m,\vee}\left(k_{(m,0),(m,\vee)}-k_{(m,0)}\right),$$

$$k_{(m,0),(m,\vee)}=\min\left(k_{m,0}+k_{m,\vee}\right),\ldots,\max\left(k_{m,0}+k_{m,\vee}\right).$$

Второй этап осуществляется путем преобразования последовательности из полученной плотности распределения вероятностей $f_{(m,0),(m,\vee)}\left(k_{(m,0),(m,\vee)}\right)$ и $f_{m,mN+1}\left(k_{m,mN+1}\right)$. Итоговая плотность распределения вероятностей времени выполнения процесса защиты информации всеми M подсистемами:

$$f_{(m,0),(m,\vee),(m,mN+1)}\left(k_{(m,0),(m,\wedge),(m,mN+1)}\right)=\sum_{\min k_{(m,0),(m,\vee)}}^{\max k_{(m,0),(m,\vee)}} f\left(k_{(m,0),(m,\vee)}\right) f_{m,mN+1}\left(k_{(m,0),(m,\vee),(m,mN+1)}-k_{(m,0),(m,\vee)}\right),$$

$$k_{(m,0),(m,\vee),(m,mN+1)}=\min\left(k_{(m,0),(m,\vee)}+k_{(m,mN+1)}\right),\ldots,\max\left(k_{(m,0),(m,\vee)}+k_{(m,mN+1)}\right),$$

где $m=1,2,\ldots,M$ – порядковый номер подсистемы,

N – номер последнего действия перед передачей результатов обработки по процессу защиты информации из подсистемы.

Введем следующее равенство:

$$f_m\left(k_m\right)=f_{(m,0),(m,\vee),(m,mN+1)}\left(k_{(m,0),(m,\vee),(m,mN+1)}\right),$$

$$k_m=k_{(m,0),(m,\vee),(m,mN+1)},$$

где $m=1,2,\ldots,M$ – порядковый номер подсистемы.

Плотность распределения времени выполнения процесса защиты информации комплексной системы защиты информации с узлом соединения параллельных подсистем на базе функции синхронизации первого уровня «V» и узлом соединения параллельных подпроцессов защиты информации

подсистем на базе функции синхронизации второго уровня «V» представляет собой:

$$f_{\vee\vee}\left(k_{1,2,\ldots,M}\right)=\prod_{m=1}^{M}\left(1-\sum_{k_{1,2,\ldots,M}=1}^{k_{1,2,\ldots,M}-1}f_m\left(k_m\right)\right)-\prod_{m=1}^{M}\left(1-\sum_{k_{1,2,\ldots,M}=1}^{k_{1,2,\ldots,M}}f_m\left(k_m\right)\right).$$

Без учёта влияния окружающей среды:

$$k_{1,2,\ldots,M}=\min\left(\min k_1,\min k_2,\min k_M\right),\ldots,\min\left(\max k_1,\max k_2,\max k_M\right).$$

С учётом влияния окружающей среды:

$$k_{1,2,\ldots,M}=\min\left(\min k_1,\min k_2,\min k_M\right)+k_t,\ldots,\min\left(\max k_1,\max k_2,\max k_M\right)+k_t,$$

где M – порядковый номер подсистемы;

k_t – дискретное время, затраченное на процесс передачи входной информации подсистеме и получение информации по результатам обработки от подсистемы.

Процесс преобразования полученной последовательности из действий $f_0\left(k_0\right)$, $f_{\vee\vee}\left(k_{\vee\vee}\right)$ и $f_{N+1}\left(k_{N+1}\right)$ выполняется в 2 этапа.

Первый этап осуществляется путем преобразования последовательности из действий, описываемых плотностями $f_0\left(k_0\right)$ и $f_{\vee\vee}\left(k_{\vee\vee}\right)$:

$$f_{0,\vee\vee}\left(k_{0,\vee\vee}\right)=\sum_{\min k_0}^{\max k_0}f\left(k_0\right)f_{\vee\vee}\left(k_{0,\vee\vee}-k_0\right),$$

$$k_{0,\vee\vee}=\min\left(k_0+k_{\vee\vee}+k_t\right),\ldots,\max\left(k_0+k_{\vee\vee}+k_t\right).$$

Второй этап осуществляется путем преобразования последовательности из полученной плотности распределения вероятностей $f_{0,\vee\vee}\left(k_{0,\vee\vee}\right)$ и $f_{N+1}\left(k_{N+1}\right)$. Итоговая плотность распределения вероятностей времени окончания процесса защиты информации всеми M подсистемами:

$$f_{0,\vee\vee,N+1}\left(k_{0,\vee\vee,N+1}\right)=\sum_{\min k_{0,\vee\vee}}^{\max k_{0,\vee\vee}}f\left(k_{0,\vee\vee}\right)f_{N+1}\left(k_{0,\vee\vee,N+1}-k_{0,\vee\vee}\right),$$

$$k_{0,\vee\vee,N+1}=\min\left(k_{0,\vee\vee}+k_{N+1}\right),\ldots,\max\left(k_{0,\vee\vee}+k_{N+1}\right),$$

где N – номер последнего действия перед передачей результатов обработки по процессу защиты информации из подсистемы.

Введем следующее равенство:

$$f_{1\vee\vee}\left(k_{1\vee\vee}\right) = f_{0,\vee\vee,N+1}\left(k_{0,\vee\vee,N+1}\right),$$

$$k_{1\vee\vee} = k_{0,\vee\vee,N+1}.$$

Математическое ожидание и дисперсия дискретного времени окончания процесса защиты информации, а также риск срыва временного регламента комплексной системы защиты информации с узлом соединения параллельных подсистем на базе функции синхронизации первого уровня «V» и узлом соединения параллельных подпроцессов защиты информации подсистем на базе функции синхронизации второго уровня «V» описываются следующим образом:

$$E\left[k_{1\vee\vee}\right] = \sum_{\min k_{1\vee\vee}}^{\max k_{1\vee\vee}} k_{1\vee\vee} f_{1\vee\vee}\left(k_{1\vee\vee}\right),$$

$$D\left[k_{1\vee\vee}\right] = \sum_{\min k_{1\vee\vee}}^{\max k_{1\vee\vee}} \left(k_{1\vee\vee} - E\left[k_{1\vee\vee}\right]\right)^2 f_{1\vee\vee}\left(k_{1\vee\vee}\right),$$

$$R\left[C\right] = \sum_{k_{1\vee\vee} > C} f_{1\vee\vee}\left(k_{1\vee\vee}\right).$$

Для сравнительного анализа различных реализаций необходима единая система формализаций, которая позволит ранжировать предлагаемые решения и с единой позиции подойти ко всем механизмам, основываясь на квалиметрических характеристиках с возможностью оценки степени доверия. Исходя из этого, образуется объективная необходимость расширения модельного ряда комплексных систем защиты.

Генерация вычислительного интеллекта и его введение в архитектуру комплексных систем защиты информации позволит обеспечить принятие решений в режиме реального времени и оперативное реагирование на возникающие угрозы в целях обеспечения высокого уровня защиты информации в соответствии с требуемой оценкой степени доверия к системе.

Список используемых источников

1. Птицын А. В., Птицына. Л. К. Генерация системно-аналитического ядра безопасных информационных технологий. СПб.: Изд-во Политехн. ун-та, 2011. 263 с.

2. Птицын А. В., Птицына Л. К. Обеспечение информационной безопасности на основе методологического базиса агентных технологий // Вестник Брянского государственного технического университета. 2017. № 2 (55). С. 146–154.

3. Птицын А. В., Птицына Л. К. Аналитическое моделирование комплексных систем защиты информации. Гамбург. Saarbrucken: LAP LAMBERT Academic Publishing, 2012. 293 с.

УДК 621.372.54
ГРНТИ 49.03.13

РАСЧЁТ ВОЛОКОННО-ОПТИЧЕСКОГО ДЕЛИТЕЛЯ МОЩНОСТИ НА ОСНОВЕ ФАЗОКОНТУРНЫХ СХЕМ ЗАМЕЩЕНИЯ

С. А. Иванов, И. Ю. Смирнов, П. Н. Федоров

Военная академия связи

В данной работе рассмотрен вопрос применения нового аналитического подхода, на основе теории синтеза оптических гетероструктур, к расчету волоконно-оптического делителя мощности, который позволит получить изделие с улучшенными техническими характеристиками. Приведен анализ применяемых сегодня технологий изготовления делителей мощности.

пассивные оптические сети, оптический делитель мощности, оптический фильтр, мультиплексор, оптический разветвитель.

Волоконно-оптические линии и сети связи на сегодняшний день занимают одно из лидирующих мест в телекоммуникационной среде. Это связано с возможностью передачи по ним большого информационного потока на больших скоростях [1]. Ведущие операторы связи прокладывают «последнюю милю» оптическим волокном. Доступ по волоконно-оптической линии связи (ВОЛС) позволяет обеспечить наилучшее качество и надежность линии связи, а также максимальную скорость доступа к информационным ресурсам. Для построения ВОЛС требуется использование специализированного активного и пассивного оборудования. Так, одним из важнейших пассивных элементов построения распределительной сети доступа PON (*Passive optical network* – пассивная оптическая сеть) является оптический разветвитель – оптический делитель мощности (рис. 1) [2].

Оптический разветвитель – это многополюсное устройство, где излучение, подаваемое на оптический вход, распределяется между многими оптическими выходами. Существует две основных технологии изготовления оптических разветвителей: сварные – Fused и планарные – PLC (*Planar Lightwave Circuit*) [3].

Сварные оптические разветвители изготовляются методом сплавления одномодовых или многомодовых оптических волокон (рис. 2а). При сплавлении двух волокон образуется X-образный оптический разветвитель 2×2, из которого можно сделать Y-образный разветвитель 1×2, удалив один из

световодов. Затухание сигнала в сплавных разветвителях составляет величину порядка 0,2...1 дБ при сохранении высокой температурной стабильности. Однако сплавной метод сложен и трудоемок, требует индивидуальной технологии изготовления каждого разветвителя.

Планарные разветвители производятся методом химического осаждения оптического материала на кремниевой поверхности в несколько слоев с вытравливанием на одной из стадии через маску планарного световода требуемой конфигурации и оптической плотности. Планарный световод находится между пластинами оптического материала и играет роль сердцевины – по нему передается оптическая мощность. Фактически создается кристалл или микросхема, состоящая из кремниевой пластины и оптических материалов, обеспечивающая равномерное разделением оптической мощности по схеме 1×2, то есть создается Y-образный оптический разветвитель. При необходимости разделения оптического сигнала по схеме больше чем один к двум, используется каскадная схема соединения делителей (рис. 2б).

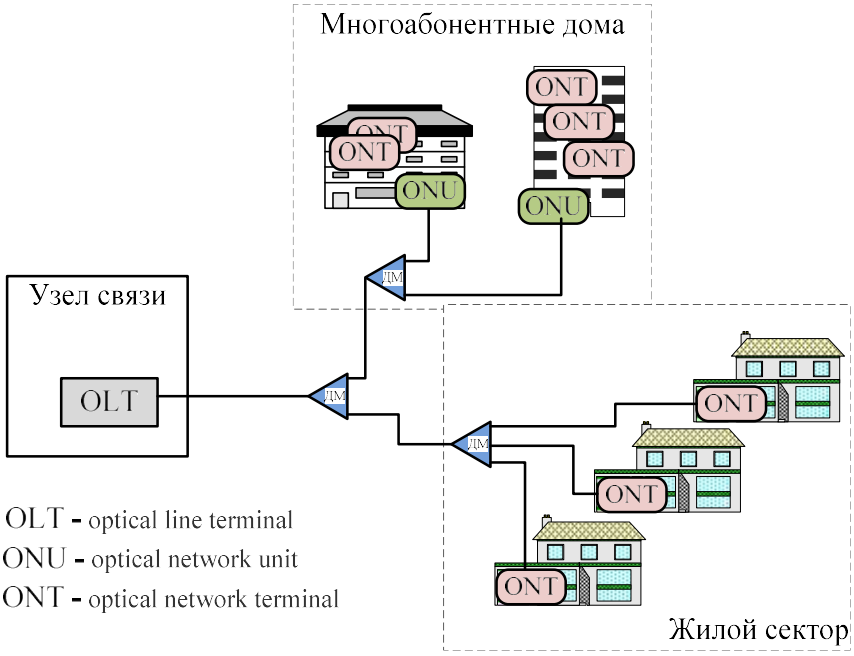


Рис. 1. Архитектура пассивной оптической сети PON

Планарные разветвители, используются на практике, в основном, для равномерного разделения оптического сигнала, так как, используя данную технологию, достаточно сложно добиться устойчивого неравномерного разделения оптической мощности.

Одним из существенных недостатков сетевой технологии PON является необходимость передачи оптического сигнала большой мощности. Это связано с тем, что при каждом разветвлении в соотношении 1:2 энергетический потенциал линии связи в среднем падает на 3,4 дБ. Следовательно, при разветвлении в соотношении 1:64 энергетический потенциал линии связи

уменьшается на 20,4 дБ. К сравнению: в одномодовом волокне потери составляют 0,3-0,4 дБ/км, в многомодовом – 0,6-1,1 дБ/км [4].

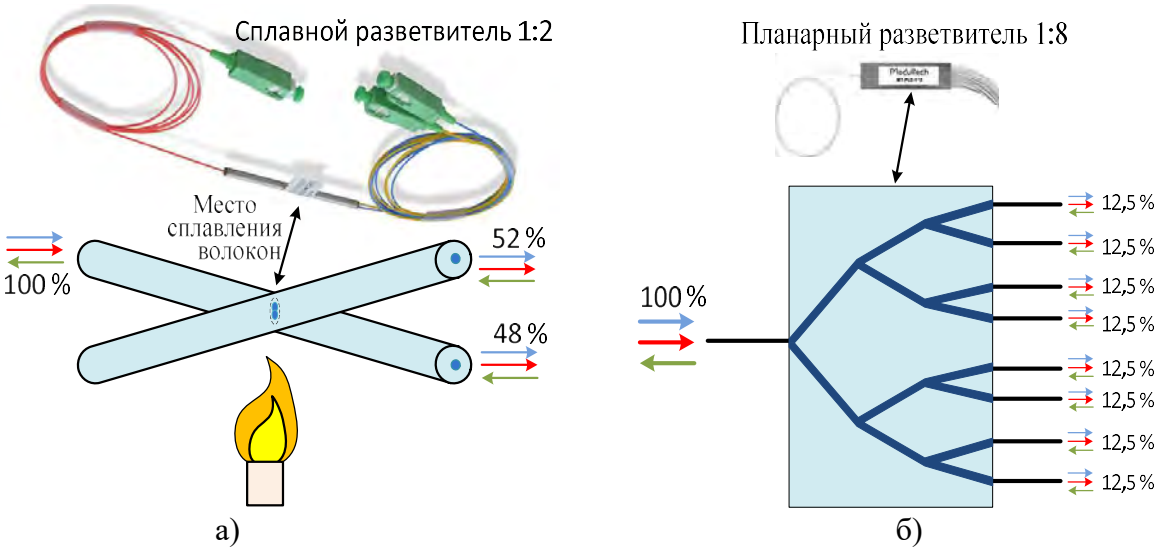


Рис. 2. Технология изготовления разветвителя:
а) сплавного, б) планарного

В наше время в обеих технологиях используется метод аппроксимации параметров, заключающейся в измерении, на стадии производства, этих параметров и доведения их до заданных значений с допустимыми погрешностями.

В данной статье предлагается новый аналитический подход к расчету необходимых параметров оптического разветвителя, который позволит получить делитель мощности с улучшенными техническими характеристиками, возможностью пропорционального деления мощности оптического сигнала с меньшими потерями.

Основой конструкции делителя является диэлектрическая пластина прямоугольного профиля со скошенным на входе торцом и зеркальной сплошной подложкой с одной стороны пластины (рис. 3). На противоположной стороне пластины крепятся оптические многослойные фильтры по заданному числу ответвлений, с расчетными значениями коэффициентов отражения и затуханий фильтров.

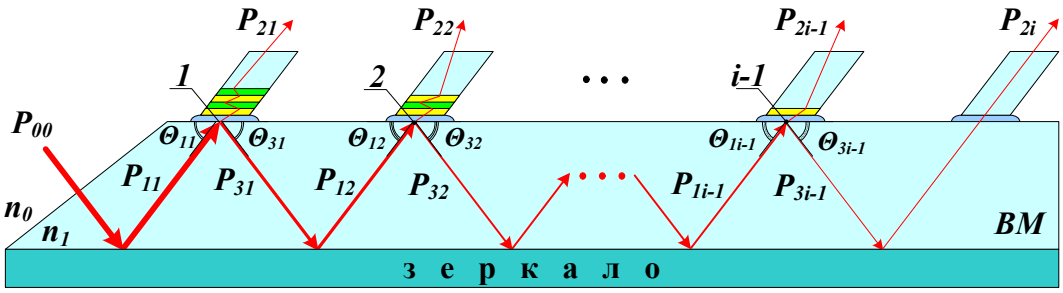


Рис. 3. Упрощенная конструкция оптического делителя мощности

На рис. 4 представлена упрощенная конструкция разветвителя в виде волнового мультиплексора (ВМ). Сигнал с мощностью P_{00} поступает из среды с показателем преломления n_0 на вход ВМ, проходит внутри пластины с показателем преломления n_1 под углом Θ_{11} и отражается от граничного слоя под углом $\Theta_{31} = \Theta_{11}$.

В точке 1 падения луча на граничный слой ВМ сигнал с мощностью P_{11} разветвляется на два направления с мощностями: P_{21} – преломленного луча и P_{31} – отраженного луча, т. е.:

$$P_{11} = P_{21} + P_{31}. \quad (1)$$

Луч отраженного сигнала, попадая на зеркало с коэффициентом отражения, близким к единице, отражается без потерь с мощностью $P_{12} = P_{31}$ и попадает в точку 2 на граничном слое пластины ВМ, где луч сигнала снова делится на два: преломленный с мощность P_{22} и отраженный луч с мощностью P_{32}, т. е.:

$$P_{12} = P_{22} + P_{32}. \quad (2)$$

В общем виде для i–го ответвления можно записать:

$$P_{1i} = P_{2i} + P_{3i}, \quad (3)$$

где по номеру ответвления $i = 1 \ldots N$.

Разделение сигнала по ответвлениям осуществляется с помощью полосовых фильтров с разными затуханиями в полосах пропускания (ППр) на одинаковой средней частоте, равной частоте разветвляемого сигнала. Ширина ППр может быть любой, но как можно шире, чтобы снизить зависимость затухания от возможного температурного ухода характеристики затухания фильтра. Тогда рабочее затухание оптического фильтра в каждом ответвлении должно быть равно:

$$a_i = 10 \lg \frac{P_{1i}}{P_{2i}}. \quad (4)$$

Из N фильтров минимальное затухание имеет фильтр в последнем N-ом ответвлении, которое при согласованном включении делителя может быть равным нулю. В остальных фильтрах затухание будет определяться в соответствии с формулой (4). Очередность расчета ОМСФ начинается с последнего (N-го) ответвления.

В *i*-х точках разветвления мощность падающей волны P_{1i} делится на две составляющие: мощность отраженной волны – P_{3i} и мощность прошедшей волны – P_{2i}, соотношения между которыми определяются формулой (2) соответствующими коэффициентами: отражения – R_i и прохождения – T_i.

Коэффициенты отражения и прохождения определяется:

$$R_i = \frac{P_{3i}}{P_{1i}}; \qquad T_i = \frac{P_{2i}}{P_{1i}} \tag{5}$$

С учетом (1) получаем соотношение между коэффициентами отражения и прохождения:

$$R_i + T_i = 1. \tag{6}$$

Коэффициент отражения мощности на входе оптического фильтра определяется через значения его характеристического сопротивления Z_{2i} на средней частоте f_0 и показателя преломления среды пластины ВМ – n_{1i}:

$$R_i = \left(\frac{n_1 - 1/z_{2i}}{n_1 + 1/z_{2i}} \right)^2. \tag{7}$$

Коэффициент прохождения мощности T_i (коэффициент передачи) определяется из (6) выражением:

$$T_i = 1 - R_i = \left(\frac{\sqrt{n_1 / z_{2i}}}{n_1 + 1/z_{2i}} \right)^2. \tag{8}$$

Величина характеристического сопротивления фильтра со стороны входа на средней частоте полосы пропускания Z_{2i} связана с рабочим затуханием фильтра Δa_i на той же частоте известной формулой:

$$Z_{21} = 10^{\Delta a/20} \pm \sqrt{10^{\Delta a/10} - 1}, \tag{9}$$

в которой знак минус относится к фильтрам с топологией типа Т и знак плюс с топологией типа П [5, 6].

Расчет оптического разветвителя включает в себя три этапа. Первый этап: определение значений мощностей на входах каждого ответвления P_{1i}, значений затухания фильтров Δa_i и характеристических сопротивлений Z_{2i} на средней частоте Второй этап: расчет оптических многослойных фильтров

(ОМСФ) с определением топологии, значений показателей преломления материала отдельных слоев, частотных характеристик затухания и характеристического сопротивления каждого фильтра. Третий этап: расчет согласующих оптических трансформаторов на входе ($ОТ_{1i}$) и выходе ($ОТ_{2i}$) фильтра в каждом ответвлении. Теоретической основой решения задачи расчета ОМСФ и трансформаторов является метод моделирования четвертьволнового отрезка линии схемой ФК1П [5, 7].

Рассмотренная методика синтеза оптических разветвителей мощности, построенных на основе волнового мультиплексора и оптических фильтров, дает возможность произвести расчет параметров передачи сигналов с заданной точностью, что очень важно в цепях регулировки уровней передачи и приема отдельных трактов и каналов при построении PON.

Список используемых источников

1. Иванов Н. А., Иванов С. А., Стахеев И. Г. Современные специализированные оптические волокна // Актуальные проблемы инфотелекоммуникаций в науке и образовании: III Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2-х т.: СПб.: СПбГУТ, 2015. Т. 2. С. 1228–1232.

2. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 5-е изд. СПб.: Питер, 2016. 992 с.

3. Гуляева Г. И. Основные элементы архитектуры пассивной оптической сети доступа PON // Инженерные кадры – будущее инновационной экономики России. 2018. № 3. С. 119–121.

4. Иванов С. А., Сапченко Е. С., Смирнов И. Ю. Применение полевых оптических кабелей в роботехнических комплексах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. Т. 1. С. 515–519.

5. Лапшин Б. А. Оптические гетероструктуры. Новая теория и расчет. СПб.: БХВ-Петербург, 2012. 480 с.: ил.

6. Иванов С. А., Иванов Н. А., Лапшин Б. А., Политыкин Р. В., Смирнов И. Ю. Способ моделирования линии связи с распределенными параметрами. Пат. 2583740 Российская Федерация; заявитель и патентообладатель Военная академия связи. – № 2015100724/08; заявл. 12.01.2015; опубл. 10.05.2015.

7. Смирнов И. Ю., Иванов С. А., Стародубцев Ю. И., Алисевич Е. А. Термостойкий интегрально-оптический делитель излучения. Пат. 2718669 Российская Федерация; заявитель и патентообладатель Смирнов И. Ю. – № 2019120478; заявл. 13.04.2020; опубл. 28.06.2019.

УДК 004.45
ГРНТИ 50.41.17

СОЗДАНИЕ ПРОГРАММНОЙ ОБЪЕКТНО-ОРИЕНТИРОВАННОЙ ПЛАТФОРМЫ ДЛЯ РАЗРАБОТКИ UEFI МОДУЛЕЙ

К. Е. Израилов[1], **В. В. Покусов**[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Казахстанская Ассоциация Информационной Безопасности

В статье рассматривается задача разработки модулей, использующих UEFI. Указываются некоторые возникающие при этом проблемные вопросы, такие, как недостаточная функциональность используемого языка C, сложность логирования операций, а также невозможность прямой отладки кода. В качестве альтернативного подхода предлагается и описывается разработанная платформа, позволяющая более удобно разрабатывать модули. К ее достоинствам относятся такие, как использование языка программирования C++ и большого набора классов-оберток над UEFI функционалом, возможность логирования действий, встроенный интерпретатор языка C для отладки в псевдо-интерактивном режиме, наличие примитивов для создания текстовых графических интерфейсов с набором окон и их стандартных элементов, а также поддержка потоковой кооперативной многозадачности. Разработка платформы является полностью авторской.

BIOS, UEFI, модуль, разработка, платформа, достоинства и недостатки, системное программное обеспечение.

Введение

Общая тенденция развития информационных технологий находит свое отражение и в таких программно-аппаратных составляющих информационных систем, как современные компьютеры и механизмы их работы. Так, на смену морально устаревшему программному обеспечению по реализации API для работы с аппаратурой компьютера и подключенными устройствами (выполняемому в начале загрузки) – BIOS [1], пришла его более новая и совершенная версия – UEFI [2], обладающая целым рядом преимуществ: драйвера устройств, графический интерфейс, б***о***льшие объемы поддерживаемой памяти, функции безопасности [3] и т. п.; впрочем, необходимо отметить, что и сам по себе UEFI продолжает оставаться не гарантированно безопасным [4]. Тем не менее, несмотря на такой прогресс в проектировании системного программного обеспечения, разработка модулей, расширяющих функционал UEFI, все также остается технически сложной задачей. Далее будут указаны основные проблемы, возникающие при создании UEFI-

модулей классическим подходом, а также описана разработанная программная объектно-ориентированная платформа, частично их разрешающая.

Проблемные вопросы разработки

Приведем наиболее яркие проблемные вопросы, возникающие при разработке модулей для UEFI [5, 6, 7].

Во-первых, если для разработки BIOS часто и использовался такой низкоуровневый язык программирования, как ассемблер, то в случае UEFI стало возможным применение всей мощи языка программирования C (например, работа с памятью через указатели, введение пользовательских структур, поддержка сложных типов переменных и т. п.) [8]. Тем не менее, поскольку UEFI, по сути, представляет собой мини операционную систему (с собственным аналогом полноценной файловой системы, драйверов и пр.), в большей степени оперирующей логическими объектами (аналогами классов в языках программирования) то такое языковое расширение разработки оказывается недостаточным (хотя и не критичным).

Во-вторых, поскольку сама суть UEFI подразумевает, что его код может выполняться до момента инициализации видеокарты или клавиатуры, или же вообще при их отсутствии, то необходимы способы отладки модулей как без ручного участия человека, так и без непосредственного наблюдения за результатом. Однако, прямая возможность этого в современных условиях отсутствует, что существенно усложняет процесс разработки.

В-третьих, сам по себе процесс отладки UEFI-модулей представляет собой трудную задачу, поскольку не всегда есть возможность подключения аппаратных отладчиков, а постепенное добавление отладочных функций в код для вывода интересующей информации занимает ощутимое время – пересборка модуля, его внедрение в UEFI-прошивку, ее загрузка в компьютер, перезапуск компьютера. При этом, если в случае ошибки разработчика компьютер перестанет загружаться (доходить до основной операционной системы), то придется применять аппаратное восстановление работающей прошивки, которое увеличит время еще больше.

Отметим, что для разрешения последних двух проблемных вопросов применяются эмуляторы, встроенные в среды разработки для UEFI. Однако, работа в них модулей будет отличаться от работы в реальных условиях (например, отсутствием полноценной эмуляции аппаратного обеспечения), что далеко не всегда допустимо. Применение же полноценных эмуляторов вида VMware возможно, но оно все также будет иметь определенные отличия от реального оборудования; также, отладка в нем UEFI (именно в первые моменты запуска виртуальной машины) будет иметь множество технических сложностей.

Предлагаемое решение

Предлагаемое решение, частично нейтрализующее указанные проблемы разработки, построено на следующих принципах.

Во-первых, решение представляет собой платформу в виде дополнительного слоя между UEFI и разрабатываемыми модулями, целью которого является упрощение проектирования, разработки и отладки.

Во-вторых, платформа (а, следовательно, и используемые ее модули) написана на высокоуровневом языке программирования C++, который превосходит язык C множеством возможностей, таких, как поддержка различных парадигм программирования (например, объектно-ориентированное и обобщенное) [9]. В частности, в ней присутствуют стандартные STL-контейнеры (список, массив, хэш и пр.), полноценный класс для работы со строками и ряд других вспомогательных библиотек. Также, реализованы классы-обертки над UEFI функционалом (например, по работе с протоколами UEFI), что за счет объектной ориентированности существенно упрощает написание и чтение исходного кода.

В-третьих, в платформу встроены механизмы логирования действий, доступные разрабатываемым модулям, что позволит их отлаживать при отсутствии возможности взаимодействия пользователя с UEFI; например, когда драйвера клавиатуры и видеокарты не загружены. Важной особенностью является то, что логи могут быть просмотрены разработчиком в специальном режиме работы платформы, когда все необходимые для этого драйвера уже будут загружены.

В-четвертых, в систему встроен интерпретатор языка C с доступом к памяти и возможностью вызова функций UEFI, которые необходимы разработчику не столько для отладки своего кода, сколько для исследования состояния загрузки компьютера (например, путем запроса состояния UEFI-протоколов, а затем получения через них списка и информации о подключенных устройствах). Впрочем, при необходимости интерпретатор может быть расширен поддержкой вызовов собственных функций модуля, таких, как специализированные процедуры тестирования. Такой режим отладки условно можно назвать *псевдо-интерактивным*.

В-пятых, платформа поддерживает общую идеологию и набор примитивов для создания многооконных и многоэлементных TUI (от *англ.* Textual User Interface, *перев.* на рус. яз. Текстовый Пользовательский Интерфейс). Последний является более совершенной версией простых интерфейсов BIOS, представляющих собой набор однотипных окон, содержащих пункты меню. При этом, дальнейшее развитие интерфейсов в сторону графических (что как правило делается при разработке под UEFI), как показывает практика, далеко не всегда востребовано и несет больше негативных последствий для удобства пользователей, чем позитивных [10]. TUI поддерживает такие элементы, как вложенные окна, меню, скроллинг пространства,

списки, таблицы, кнопки, окна редактирования, файловый браузер и пр. [11, 12].

В-шестых, платформа поддерживает потоковую кооперативную многозадачность на уровне отдельных функций с привязкой к счетчику времени [13]. Таким образом, возможна реализация полноценных динамических операций, одновременно выводящих на экран свои статусы, прогресс и прочую информацию.

И, в-седьмых, сборка и отладка исходного кода осуществляется в среде разработки Microsoft Visual Studio (используя собственные утилиты компиляции, ассемблирования и линковки), что, безусловно повышает удобство работы по сравнению, например, с использованием текстового редактора и консольного отладчика.

Заключение

В статье были приведены основные моменты классического подхода при написании программ, использующих UEFI, и возникающие при этом проблемные вопросы. Разработанная авторами платформа позволяет реализовывать модули более простым образом за счет частичного нивелирования этих вопросов. Данный продукт в некотором роде можно считать прочно занимающим частично пустующую нишу между устаревающими простыми текстовыми реализациями BIOS и чрезмерно нагруженными графическими модулями для UEFI. Продолжением исследования и разработки должно стать наращивание платформы новым современным функционалом (например, в части сетевой поддержки) и еще большим упрощением механизмов отладки. Также, крайне актуальной может считаться задача наращивания функционала платформы для обеспечения информационной безопасности ресурсов компьютера [14], включая проверку безопасности программного обеспечения [15, 16, 17, 18] операционной системы еще до ее загрузки.

Список используемых источников

1. Steers K. Inside the bios // PC World. 2002. Т. 20. № 6. С. 84.

2. Денисов А. А., Черноусов И. А. Технология UEFI – перспективы и проблемы // Машиностроитель. 2012. № 7. С. 32–33.

3. Покусов В. В., Кожамкулов М. С. Возможности UEFI для реализации функций защиты информации // Аллея науки. 2018. Т. 1. № 10 (26). С. 456–461.

4. Васильева К. В., Коноплев А. С. Метод анализа встроенного программного обеспечения UEFI BIOS на предмет наличия НДВ // Методы и технические средства обеспечения безопасности информации. 2019. № 28. С. 34–35.

5. Кашубина А. П., Иванов А. П. Подходы к реализации модуля доверенной загрузки для вычислительной платформы с технологией UEFI // Инжиниринг и технологии. 2017. Т. 2. № 2. С. 19–23.

6. Чеботарёв С. И., Косолапов А. А., Сергеев А. В., Башун В. В. UEFI-драйвер контроля клавиатуры как средство для тестирования модулей доверенной загрузки // Научная сессия ГУАП. сборник докладов: Санкт-Петербургского государственного университета аэрокосмического приборостроения (Санкт-Петербург, 2016). 2016. С. 314–317.

7. Тищенко Е. Н., Буцик К. А., Деревяшко В. В. Модель доверенной сетевой загрузки «Тонкого клиента» с нейтрализацией «внутреннего нарушителя» // Известия ЮФУ. Технические науки. 2015. № 5 (166). С. 37–47.

8. Дорофеева О. С., Казаков Б. В., Казакова И. А. Методика перехода от языка программирования паскаль к языку программирования Си // Проблемы автоматизации и управления в технических системах: сборник статей XXXII Международной научно-технической конференции (Пенза, 2017). 2017. С. 316–317.

9. Ускова О. Ф., Каплиева Н. А. Расширение возможностей функций в языке программирования С++ по сравнению с языком программирования Паскаль // Информатика: проблемы, методология, технологии: сборник материалов XIX международной научно-методической конференции (Воронеж, 2019). 2019. С. 1827–1829.

10. Корпан Л. М. Признаки культурного феномена в дизайне графических пользовательских интерфейсов // Вестник Волгоградского государственного университета. Серия 7: Философия. Социология и социальные технологии. 2016. № 1 (31). С. 130–136.

11. Курта П. А. Взаимодействие пользователя с информационной системой. Часть 1. Схема взаимодействия и классификация недостатков // Известия СПбГЭТУ ЛЭТИ. 2020. № 8-9. С. 35–45.

12. Курта П. А. Взаимодействие пользователя с информационной системой. Часть 2. Алгоритмы обнаружения недостатков // Известия СПбГЭТУ ЛЭТИ. 2020. № 10. С. 34–44.

13. Курниц А. Freertos – Операционная система для микроконтроллеров // Компоненты и технологии. 2011. № 5 (118). С. 97–102.

14. Буйневич М. В., Израилов К. Е. Аналитическое моделирование работы программного кода с уязвимостями // Вопросы кибербезопасности. 2020. № 3 (37). С. 2–12.

15. Буйневич М. В., Израилов К. Е. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 1. Функциональная архитектура // Информационные технологии и телекоммуникации. 2016. Т. 4. № 1. С. 115–130.

16. Израилов К. Е. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 2. Информационная архитектура // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 86–104.

17. Израилов К. Е., Покусов В. В. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 3. Модульно-алгоритмическая архитектура // Информационные технологии и телекоммуникации. 2016. Т. 4. № 4. С. 104–121.

18. Buinevich M., Izrailov K. Method and utility for recovering code algorithms of telecommunication devices for vulnerability search // The Proceedings of 16th International Conference on Advanced Communication Technology (ICACT 2014). 2014. Pp. 172–176.

УДК 621.391
ГРНТИ 81.93.29

К ВОПРОСУ ОБ ИЗМЕНЕНИЯХ В СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ В ОПЕРАЦИОННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

О. Б. Ильина[1], **О. П. Купчиненко**[1], **А. В. Скоропад**[2]

[1]Военная академия связи
[2]Санкт-Петербургский филиал «Ленинградское отделение научно-исследовательского института радио»

Проведен анализ отличий в системе защиты информации в операционной системе специального назначения Astra Linux SE Смоленск, версия 1.6. Рассмотрена мандатная сущностно-ролевая модель управления доступом и информационными потоками, которая содержит дополнительные способы разграничения доступа. Проанализированы особенности применения режима мандатного контроля целостности.

операционная система специального назначения, защита информации, мандатная модель разграничения доступа, мандатный контроль целостности, привилегии.

В современных условиях возрастает роль информационных технологий, расширяется сфера применения автоматизированных систем специального назначения (АС СН) в процессах управления. В связи с этим необходимо уделять повышенное внимание вопросам обеспечения безопасности информации. Основой построения современных АС СН, надежных и функционально устойчивых, является использование доверенной программно-аппаратной платформы (среды).

В настоящее время операционная система специального назначения (ОС СН) Astra Linux SE, является оптимальной платформой для создания отечественной защищенной ОС СН. Наличие в данной ОС СН большого набора сертифицированных средств защиты информации и применение их в комплексе создает основу для проведения работ по созданию надежной, гибкой и многофункциональной системы защиты информации (СЗИ) в АС СН [1, 2].

Вместо системы принудительного контроля доступа, в ОС СН Astra Linux SE (начиная с версии 1.5), используется мандатная сущностно-ролевая модель управления доступом (МРОСЛ ДП-модель). Эта модель лишена недостатков предыдущих моделей (деклассификация, нарушение логики доступа к данным при обработке потока информации в распределенной среде) и содержит дополнительные способы разграничения доступа [3].

ДП-модель отличается от классической модели мандатного управления доступом, в ней дополнительно реализован мандатный контроль целостности (МКЦ) дистрибутива и файловой системы, предусмотрено ролевое управление доступом и реализовано применение противодействия запрещённым потокам по памяти и времени.

В ОС СН Astra Linux SE Смоленск, версия 1.6, представлены следующие отличия в СЗИ:

– после установки ОС (по умолчанию) включен режим МКЦ, параметр ядра max_ilev = 63, все процессы имеют МКЦ = 63;

– графический сервер работает от пользователя ОС СН (по умолчанию) на выделенном уровне МКЦ = 8, права суперпользователя игнорируются;

– после установки ОС СН МКЦ на файловую систему (ФС) по умолчанию выключен, но должен быть включен после настройки ОС администратором;

– в системе мандатного разграничения доступа (МРД) настроено 4 уровня конфиденциальности (0–3), количество уровней можно увеличить до 255;

– при входе через консоль или графический интерфейс (по умолчанию) суперпользователь, созданный при установке ОС, получает МКЦ=63, «красный» уровень (при входе суперпользователя предусмотрен диалог для выбора значений мандатных атрибутов), обычные пользователи получают нулевой «синий» уровень МКЦ;

– при входе через SSH (*Secure Shell*) (по умолчанию) автоматически МКЦ = 63 для администраторов из группы astra-admin (диалог выбора значений мандатных атрибутов при входе не предусмотрен), пользователи получают нулевой «синий» уровень МКЦ;

– для отдельных служб можно задать свой определенный уровень МКЦ, так же можно задать для службы systemd свой уровень конфиденциальности;

– после включения МКЦ на ФС службы или процессы на определенном уровне МКЦ (например, МКЦ = 1 или 2) не смогут записывать данные в файлы и каталоги, на которых максимальное значение МКЦ = 63.

Для сетевых сервисов рекомендуется МКЦ = 1, для подсистем виртуализации (для гостевых систем, отличных от ОС СН Astra Linux Special Edition Смоленск) МКЦ = 2, для внешнего специального программного обеспечения (СПО) МКЦ = 3;

– X-сервер по умолчанию работает от имени пользователя fly-dm МКЦ = 8;

– при установке системы следующим устройствам: dev/sd*, /dev/vd*, /dev/hd*, автоматически присваивается уровень конфиденциальности МКЦ = 3.

Изменения для мандатных атрибутов ccnr, ccnri, ehole представлены в таблице.

ТАБЛИЦА. Мандатные атрибуты

Атрибут	Изменения
ccnr	Разрешена установка на контейнеры
ehole	Запрещена установка на контейнеры Разрешена установка только на файлы
ccnri	Разрешена установка на контейнеры Включен при установке обновлений безопасности версии 1.6 для всех каталогов
whole	Новый атрибут Разрешает записывать в файл «снизу вверх» (чтение по обычным правилам МРД). Запрещена установка на контейнеры

Запись в каталог с высокой целостностью не может быть выполнена процессом с более низким уровнем целостности, чем у контейнера.

Пользователь не может производить запись в контейнер (каталог) с установленным МКЦ>0 в следующих случаях:

– пользователь не вошел в систему на уровне МКЦ > уровня МКЦ контейнера;

– пользователь не обладает привилегией parsec_cap_ignmacint.

Пользователь не может производить запись в контейнер (каталог) с установленной (ненулевой) меткой конфиденциальности и с установленным флагом ccnr информации, отличной от уровня конфиденциальности контейнера в следующих случаях:

- Пользователь не зашел под уровнем конфиденциальности равным уровню конфиденциальности контейнера (каталога).
- Пользователь не обладает привилегиями parsec_cap_ignmaccat и parsec_cap_ignmaclvl.

Пользователь, который не обладает никакими привилегиями, может производить запись файлов с любым уровнем конфиденциальности, не больше уровня конфиденциальности каталога, в каталог с установленным атрибутом ccnr, если в загрузчике указан параметр ядра parsec.ccnr_relax = 1.

Уровни целостности субъекта и объекта сравнивают по битовой маске. Запись в объект разрешается, если для субъекта набор бит уровня МКЦ «включает» в себя набор бит уровня МКЦ объекта.

После установки контроля целостности на ФС максимальный уровень целостности (по умолчанию 63) будет установлен на следующие каталоги: /etc, /lib, /lib64, /lib32, /bin, /sbin, /boot, /root, /opt, /srv, /usr.

В СЗИ добавлены новые Parsec-привилегии:

– PARSEC_CAP_IPC_OWNER отменяет мандатные ограничения при работе с объектами IPC (*Inter Process Communications* – межпроцессное взаимодействие), такими как shared memory, message queue и т. д.;

– PARSEC_CAP_BYPASS_KIOSK разрешает игнорировать ограничения Киоска [4];

– PARSEC_CAP_SUMAC разрешает запускать процессы с другим уровнем конфиденциальности.

Привилегия предыдущих версий ОС СН Astra Linux Special Edition Смоленск PARSEC_CAP_UNSAFE_SETXATTR позволяет устанавливать мандатные атрибуты объектов ФС без учета мандатных атрибутов родительского контейнера. Используется для восстановления объектов ФС из резервных копий.

Данные изменения в ОС СН Astra Linux SE Смоленск, версия 1.6, позволяют построить такую СЗИ, при работе с которой случайное или преднамеренное нарушение безопасности информационных ресурсов в АС СН под управлением ОС Astra Linux SE сведено к минимуму.

Список используемых источников

1. Гринь Д. В., Ильина О. Б., Купчиненко О. П., Скоропад А. В. Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения Astra Linux SE // Региональная информатика и информационная безопасность: сб. тр. СПб.: СПОИСУ, 2017. Вып. 4. С. 76–78.

2. Ильина О. Б., Купчиненко О. П., Скоропад А. В. О дополнительных задачах администрирования средств защиты информации в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2019. Т. 2. С. 318–323.

3. Буренин П. В., Девянин П. Н. и др. Безопасность операционной системы специального назначения Astra Linux Special Edition: учеб. пособие. М.: Горячая линия – Телеком, 2018. 311 с.

4. Ильина О. Б., Купчиненко О. П., Скоропад А. В. К вопросу о дополнительных средствах защиты информации в операционной системе специального назначения «Astra Linux SE» // Информационная безопасность регионов России: материалы XI Санкт-Петербургской международной конференции, СПб, 23-25 октября 2019 г. СПб.: СПОИСУ, 2019. Т.2. С. 224–226.

УДК 621.391
ГРНТИ 81.93.29

О ЗАЩИЩЕННОМ КОМПЛЕКСЕ ПРОГРАММ ЭЛЕКТРОННОЙ ПОЧТЫ ИЗ СОСТАВА СОВРЕМЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

О. Б. Ильина[1], **О. П. Купчиненко**[1], **А. В. Скоропад**[2]

[1]Военная академия связи
[2]Санкт-Петербургский филиал «Ленинградское отделение научно-исследовательского института радио»

Проведен анализ состава защищенного комплекса программ электронной почты в среде операционной системы специального назначения Astra Linux SE. Рассмотрены механизмы повышения безопасности почтовой переписки. Проанализированы вопросы применения программных средств шифрования и создания электронной цифровой подписи в почтовых сообщениях.

операционная система специального назначения, электронная почта, сервер электронной почты, клиент электронной почты, открытый ключ, закрытый ключ. шифрование, цифровая подпись.

Решение задачи обмена сообщениями электронной почты в операционной системе специального назначения (ОС СН) Astra Linux SE реализовано на основе защищенного комплекса программ электронной почты.

В состав защищенного комплекса программ электронной почты входят сервер электронной почты, состоящий из агента передачи электронной почты Exim4 (*EXperimental Internet Mailer*) и агента доставки электронной почты Dovecot, а также клиент электронной почты Mozilla Thunderbird, обеспечивающие следующие функциональные возможности (рис. 1):

– интеграции с ядром операционной системы и с базовыми библиотеками для обеспечения мандатного разграничения доступа к почтовым сообщениям, хранящимся с использованием формата Maildir;

– автоматической маркировки создаваемых пользователем почтовых сообщений с использованием его текущего мандатного контекста.

В ОС СН «Astra Linux SE» компоненты почтового сервера представляют собой отдельные программы, и настраивать их взаимодействие нужно самостоятельно.

Для обеспечения безопасности почтовой переписки пользователи электронной почты создаются в домене Astra Linux (ALD – *Astra Linux Domain*).

Служба Astra Linux Directory (ALD) представляет собой систему управления Единым Пространством Пользователя (ЕПП) [1].

Рис. 1. Функциональные возможности защищенного комплекса программ электронной почты

Наряду с локальной работой пользователя на рабочей электронной вычислительной машине (ЭВМ) под управлением ОС СН Astra Linux SE имеется возможность организации домена Astra Linux (ALD – *Astra Linux Domain*).

При этом под ALD в общем случае понимается одна и более рабочих ЭВМ пользователей, а также специально выделенная ЭВМ, выполняющая функции первичного контроллера домена (PDC – *Primary Domain Controller*). Все ЭВМ, входящие в домен, работают в едином сетевом сегменте.

Благодаря наличию контроллера домена появляется возможность организации централизованного хранилища учетных записей пользователей домена, а также, при необходимости, централизованного защищенного файлового сервера, содержащего сетевые рабочие директории пользователей домена.

Установка службы ALD может осуществляться как при начальной установке ОС СН путем выбора соответствующих пунктов в программе установки, так и в ручном режиме уже в работающей системе.

Без установки пакетов расширения совместно с соответствующими основными пакетами невозможна централизация хранения атрибутов системы защиты информации (СЗИ) в распределенной сетевой среде, что может привести к невозможности входа пользователей в систему.

После создания мандатных атрибутов домена на сервере ALD, можно создавать пользователей домена и присваивать им наряду с дискрецион-

ными атрибутами разграничения доступа к объектам домена, мандатные атрибуты [2, 3]. Администрирование ALD можно выполнять в командной строке и с помощью графической утилиты «Доменная политика безопасности».

В состав дистрибутива ОС СН Astra Linux SE включен графический клиент электронной почты Thunderbird, позволяющий читать и отправлять письма без использования WEB-браузера. При установке системы клиент Thunderbird устанавливается автоматически.

Thunderbird это почтовый клиент Mozilla Thunderbird, кроссплатформенная программа для работы с электронной почтой и группами новостей.

Для повышения безопасности и приватности почтовой переписки в клиенте Thunderbird можно реализовать защитное преобразование электронной почты.

Для этого используются пакеты Gnu Privacy Guard (GPG) (входит в дистрибутив и устанавливается по умолчанию) и Enigmail – плагин для почтового клиента Thunderbird, обеспечивающий взаимодействие с GPG.

GPG – бесплатная программа с открытым кодом, предназначенная для шифрования, расшифровки и создания цифровой подписи (как для текстовых сообщений, так и для файлов). Она также позволяет управлять открытыми и закрытыми ключами, необходимыми для этой задачи.

Enigmail – дополнение к Thunderbird, которое позволяет работать с шифровальными возможностями GPG прямо из Thunderbird.

Программа GPG основана на принципе криптографии с открытым ключом. Каждый пользователь создает собственную пару ключей (открытый и закрытый ключи). Эту пару ключей можно использовать для шифрования, расшифровки и цифровой подписи [4].

Открытый ключ можно передавать почтовым корреспондентам. Он не подходит для чтения защищенных сообщений или для их подписывания. С помощью открытого ключа другие пользователи будут готовить сообщения для вас. Прочитать эти сообщения сможет только обладатель парного закрытого ключа.

Закрытый ключ должен храниться в надежном месте. Тот, кто владеет закрытым ключем, имеет возможность читать письма, защищенные парным ему открытым ключом. С помощью этого же ключа можно подписывать отправляемые сообщения. Закрытый ключ защищен паролем, введённым при его создании.

GPG и Enigmail позволяют прикреплять к сообщениям цифровые подписи. Если первый пользователь подписывает сообщение с помощью секретного ключа, то любой пользователь, у кого есть копия открытого ключа первого пользователя, сможет проверить подпись и убедиться, что сообще-

ние было действительно отправлено им и добралось до назначения без искажений. И наоборот, если у пользователя есть открытый ключ другого пользователя, он можете проверять его цифровые подписи.

Enigmail применяет защитное преобразование только к содержанию письма. Не будут защищены:

– тема сообщения;

– адреса получателя и отправителя, а также имена, связанные с этими адресами.

Дополнительно, при работе в клиенте Thunderbird, рекомендуется отключить возможность показа писем в формате HTML. Просмотр писем в HTML может создать определенные уязвимости, используемые для атак на веб-браузеры. Кроме того, составление писем в HTML не позволяет корректно работать шифрованию в программе GPG.

Список используемых источников

1. Деньжонков К. А., Кий А. В. и др. Основы построения и администрирования защищенной операционной системы специального назначения Astra Linux Special Edition: учеб. пособие. СПб.: ВАС, 2019, 288 с.

2. Гринь Д. В., Ильина О. Б., Купчиненко О. П., Скоропад А. В. Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения Astra Linux SE // Региональная информатика и информационная безопасность: сб. тр. СПб.: СПОИСУ, 2017. Вып. 4. С. 76–78.

3. Ильина О. Б., Купчиненко О. П., Скоропад А. В. О механизмах дискреционного разграничения доступа в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2018. Т. 2. С 356–360.

4. Ильина О. Б., Купчиненко О. П., Скоропад А. В. К вопросу о дополнительных средствах защиты информации в операционной системе специального назначения «Astra Linux SE» // Информационная безопасность регионов России: материалы XI Санкт-Петербургской межрегиональной конференции, СПб, 23–25 октября 2019 г. СПб.: СПОИСУ, 2019. Т. 2. С. 79–81.

УДК 621.391
ГРНТИ 81.93.29

РАЗГРАНИЧЕНИЕ ДОСТУПА К ДАННЫМ В СУБД ИЗ СОСТАВА ОПЕРАЦИОННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

О. Б. Ильина[1], **О. П. Купчиненко**[1], **А. В. Скоропад**[2]

[1]Военная академия связи
[2]Санкт-Петербургский филиал «Ленинградское отделение научно-исследовательского института радио»

Проанализированы особенности администрирования баз данных в операционной системе специального назначения «Astra Linux SE». Проведен анализ механизмов разграничения доступа, реализованных в защищенной СУБД PostgreSQL в операционной системе специального назначения «Astra Linux SE». Рассмотрены средства управления мандатными и дискреционными правами разграничения доступа в СУБД PostgreSQL.

операционная система специального назначения, система управления базами данных, мандатная модель разграничения доступа, дискреционная модель разграничения доступа.

Система управления базами данных (СУБД) PostgreSQL в операционной системе специального назначения «Astra Linux Special Edition» с встроенными средствами защиты информации предназначена для создания информационных и управляющих систем. Системы работают как с конфиденциальной информацией, так и с информацией, содержащей сведения, составляющие государственную тайну.

СУБД PostgreSQL поддерживает современные технологии формирования, хранения и управления данными на основе реляционной модели данных, включает стандартные и расширенные инструкции языка SQL, процедуры, вложенные запросы, управление транзакциями, расширенный состав типов хранимых данных и применение типов данных, определенных пользователем. СУБД PostgreSQL обеспечивает хранение и работу с документами формата XML.

Состав СУБД PostgreSQL:

– сервер;

– утилиты администрирования для контроля целостности, функционирования, резервного копирования и восстановления баз данных (БД), средства управления схемами данных;

– прикладные программы для доступа к БД (для расширения возможностей сервера).

СУБД PostgreSQL поддерживает конфиденциальности хранимых данных:

– защищенность по третьему классу защиты информации от несанкционированного доступа для средств вычислительной техники (СВТ) и по второму уровню контроля отсутствия недекларированных возможностей согласно требованиям руководящих документов по защите информации;

– идентификация и аутентификация субъектов доступа для получения доступа к БД централизованными средствами управления доступа ОС СН «Astra Linux Special Edition»;

– дискреционное разграничение доступа субъектов доступа к объектам БД;

– мандатное разграничение доступа субъектов доступа к объектам БД.

В качестве защищенной СУБД в составе операционной системы специального назначения (ОС СН) «Astra Linux SE Смоленск 1.6» используется СУБД PostgreSQL, версия 9.6.

В СУБД реализуется мандатная сущностно-ролевая ДП-модель управления доступом и информационными потоками [1]. В модели представлены все возможности дискреционного, мандатного и ролевого управления доступом с учетом безопасности потоков информации.

СУБД PostgreSQL обеспечивает поддержку модуля безопасности PARSEC ОС СН «Astra Linux SE», который реализует разграничение доступа на основе дискреционной и мандатной политик разграничения доступа [2, 3]. Благодаря такой поддержке в рамках инфологической и физической моделей данных возможно разграничение доступа на уровне, как схемы данных, так и таблиц базы данных (включая отдельные записи или группы записей), а также SQL-функций обработки этих записей.

Мандатное разграничение доступа позволяет реализовать многоуровневую защиту и обеспечивает разграничения доступа пользователей к защищаемым ресурсам БД и управление информационными потоками.

Мандатное разграничение доступа поддерживается для схем, таблиц, записей и функций. Дискреционное разграничение доступом поддерживается для схем, таблиц, полей и функций (табл.).

В СУБД PostgreSQL нет собственных средств работы с метками пользователей. СУБД использует для работы с метками средства ОС СН. В ОС СН «Astra Linux SE», начиная с версии 1,5, вводится понятие объектов-контейнеров (каталогов, которые могут содержать другие объекты) дополнительно к мандатной метке конфиденциальности.

Мандатный атрибут CCR (*Conteiner Clearance Required*) используется для задания способа доступа к объектам внутри контейнеров. Когда CCR установлен, доступ к контейнеру и его содержимому определяется его мандатной меткой, иначе, доступ к контейнеру разрешен, и уровень конфиденциальности контейнера не учитывается. Так же накладываются ограничения

на мандатную метку объекта: она не должна превышать метку контейнера, в котором объект содержится.

ТАБЛИЦА. Уровни поддержки дискреционной и мандатной моделей разграничения доступа в СУБД PostgreSQL в ОС СН «Astra Linux SE»

Объекты и метаданные	Дискреционное разграничение доступа	Мандатное разграничение доступа
База данных	+	+
Схема данных	+	+
Таблица	+	+
Поле (столбец)	+	-
Запись	-	+
Функция	+	+

Для назначения меток данных, в первую очередь должны быть заданы максимальные метки соответствующих объектов, например: таблиц, схем, БД.

Главный контейнер – табличное пространство pg_global, которое создается на кластер БД. Кластер является совокупностью ролей, БД и табличных пространств.

Применение мандатных прав доступа осуществляется на уровне доступа к объектам БД и на уровне доступа непосредственно к данным (на уровне записей).

Проверка мандатных и дискреционных прав доступа к объектам осуществляется одновременно, после разработки плана запросов, перед его выполнением, когда все необходимые для проверки данные и проверяемые объекты уже определены. В результате, доступ предоставляется только при одновременном разрешении его дискреционными правами разграничения доступа (ПРД).

Проверка мандатных прав доступа к записям таблиц осуществляется во время выполнения запроса.

Для администратора БД мандатное управление доступом игнорируется, администратор может производить регламентные работы с БД (например, резервное копирование и восстановление данных), т. к. данные работы требуют установки меток, уже сохраненных ранее.

Для управления дискреционными и мандатными ПРД в ОС СН «Astra Linux SE» используются следующие графические утилиты:

– PgAdmin III («Средство администрирования СУБД PostgreSQL») – программное средство проектирования БД и управления БД;

– fly-admin-smc («Управление политикой безопасности») – утилита управления протоколированием, мандатными атрибутами и привилегиями пользователей, работа с пользователями и группами.

Для управления мандатными ПРД в режиме командной строки используются следующие утилиты:

- pdp-ulbls – управление допустимыми мандатными уровнями и категориями пользователей ОС СН;
- userlev – изменение БД мандатных уровней;
- usercat – изменение БД мандатных категорий.

Для управления дискреционными правами в режиме командной строки используются утилиты:

- chown – изменение владельца и/или группы согласно заданным атрибутам;
- chmod – изменение прав доступа указанного объекта.

Администрирование БД в СУБД PostgreSQL является достаточно ресурсоемким [4]. Так для назначения мандатных меток объектам СУБД PostgreSQL необходимо запустить утилиту «pgAdmin3», а для назначения мандатных атрибутов субъектам (пользователям) необходимо запустить «fly-admin-smc». При этом в случае необходимости более детальной настройки политики разграничения доступа или проверки корректности работы СУБД, необходимо запустить утилиту «psql» – интерактивный терминал PostgreSQL. В результате, администратор обеспечения безопасности информации имеет высокую вероятность совершения ошибки.

Кроме того, требуется многократное повторения рутинных операций, таких как:

– назначение мандатных атрибутов пользователю;

– назначение мандатных меток, каждому объекту СУБД, к которому имеет доступ пользователь (БД, таблицам, записям в таблицах, столбцам в таблицах, каждой ячейке таблицы);

– настройка доступа пользователя ко всем объектам СУБД.

В защищенной СУБД PostgreSQL в среде ОС СН «Astra Linux SE» реализуются все аспекты дискреционного и мандатного управления доступом. В СУБД возможно разграничение доступа на уровне, как схемы данных, так и таблиц базы данных (включая отдельные записи или группы записей), а также SQL-функций обработки этих записей. Решением проблем администрирования БД является разработка нового программного обеспечения, которое позволит объединить функциональные возможности таких утилит, как «pgAdmin3», «fly-admin-smc» и «psql», при назначении мандатных и дискреционных атрибутов объектам и субъектам СУБД PostgreSQL в составе ОС СН «Astra Linux SE».

Новое программное обеспечение позволит не только увеличить скорость работы пользователей и минимизировать ошибки, но и понизить требования к характеристикам вычислительной техники.

Применение СУБД PostgreSQL для создания БД в интересах должностных лиц, механизмов разграничения доступа к данным позволяют решать задачи быстрого поиска информации должностными лицами, создать многоуровневую защиту с обеспечением разграничения доступа пользователей к защищаемым ресурсам БД и управлением потоками данных.

Список используемых источников

1. Буренин П. В., Девянин П. Н. и др. Безопасность операционной системы специального назначения Astra Linux Special Edition: учеб. пособие. М.: Горячая линия – Телеком, 2018. 311 с.

2. Гринь Д. В., Ильина О. Б., Купчиненко О. П., Скоропад А. В. Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения Astra Linux SE // Региональная информатика и информационная безопасность: сб. тр. СПб.: СПОИСУ, 2017. Вып. 4. С. 76–78.

3. Ильина О. Б., Купчиненко О. П., Скоропад А. В. О механизмах дискреционного разграничения доступа в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2018. Т. 2. С. 356–360.

4. Ильина О. Б., Купчиненко О. П., Скоропад А. В. Механизмы разграничения доступа к данным в СУБД в среде операционной системы специального назначения Astra Linux SE. Региональная информатика: материалы XVII Санкт-Петербургской международной конференции, СПб, 28–30 октября 2020 г. СПб: СПОИСУ, 2020. Т. 1. С 79–81.

УДК 621.004
ГРНТИ 49.33.29

СЕТЕВАЯ СЛУЖБА АУТЕНТИФИКАЦИИ

О. Б. Ильина[1], О. П. Купчиненко[1], А. В. Скоропад[2]

[1]Военная академия связи
[2]Санкт-Петербургский филиал «Ленинградское отделение научно-исследовательского института радио»

Проведен анализ особенностей сетевого протокола аутентификации Kerberos, который ориентирован на клиент-серверную модель и обеспечивает высокий уровень безопасности информации. Рассмотрены терминология и принцип работы протокола Kerberos, который позволяет передавать данные через незащищённые сети для безопасной идентификации пользователей и обеспечивает взаимную аутентификацию. Проанализированы аспекты администрирования Kerberos в операционной системе специального назначения «Astra Linux SE».

аутентификация, сетевая служба аутентификации, операционная система, протокол Kerberos, клиент-серверная модель, билет, центр распределения ключей, область, домен, принципал.

Аутентификация или проверка подлинности представляет собой один из важных компонентов любой современной операционной системы специального назначения. Задача аутентификации состоит в том, чтобы удостовериться, что пользователь действительно является тем, за кого себя выдает, поэтому если речь идет о защите информации, то аутентификация заслуживает при этом особого внимания.

Kerberos – сетевая служба аутентификации, которая основана на одноименном протоколе аутентификации. Kerberos в первую очередь является протоколом, а не системой аутентификации. Его реализации используются в различных операционных системах как метод аутентификации пользователей в домене [1]. Он ориентирован на клиент-серверную модель и предлагает механизм взаимной аутентификации (оба пользователя через сервер подтверждают личности друг друга) перед установлением связи между ними. Также учитывается тот факт, что начальный обмен информацией происходит в незащищенной среде, а передаваемые пакеты могут быть перехвачены и модифицированы.

Протокол Kerberos использует централизованное хранение аутентификационных данных и возможности использования единой учетной записи пользователя для доступа к любым ресурсам области, что является основой для построения механизмов технологии единого входа SSO (*Single Sign-On*).

Протокол Kerberos обеспечивает высокий уровень безопасности, а его преимуществом является то, что ни пароли, ни значения хеша паролей в открытом виде не передаются при любых взаимодействиях.

Kerberos не делает никаких предположений о защищённости той сети, поверх которой он работает (он просто ей не доверяет), но, предполагает, что хосты приложений и особенно хост, на котором работает центр распределения ключей KDC (*Key Distribution Center*), являются защищёнными.

Особенности Kerberos:

1. Считается, что сетевой трафик может быть прослушан, т.е. может произойти любой несанкционированный доступ к информации, поэтому удостоверяющие данные или пароли никогда не пересылаются по сети.

2. Удостоверяющие данные никогда не сохраняются на том хосте, который пользователь использует для входа. После первоначального обмена в рамках аутентификации, хост должен забыть сведения о пароле. Вся информация о удостоверяющих данных или паролях хранится в центре

распределения ключей Kerberos, который является единственном защищённым местом.

3. Любому, кто запрашивает данные, серверы приложений и хосты должны быть в состоянии подтвердить свою идентификационную сущность.

4. С помощью различные симметричных алгоритмов шифрования все коммуникации между сервисами приложений и аутентифицированными пользователями должны иметь возможность быть зашифрованными.

Аутентификация через Kerberos является фактическим стандартом аутентификации доменных пользователей и применяется в Windows Active Directiry, Samba AD DC, FreeIPA, Astra Linux Directory (ALD).

В Linux-системах существуют две основные реализации Kerberos – Heimdal и MIT. В ОС Astra Linux SE используется MIT Kerberos.

Протокол Kerberos основан на понятии Ticket (билет).

Билет (Ticket) – зашифрованный пакет данных, выдаваемый клиенту центром распределения ключей KDC для аутентификации на сервере, на котором располагается необходимая служба. Клиентский хост, как и другие промежуточные хосты, просто передают эти билеты на конечный пункт назначения, т. к. для них билет – это неразбираемый набор бит.

В Kerberos билеты могут быть:

– билетами на получение разрешения TGT (*Ticket Granting Tickets*), которые представляют собой доказательства успешно пройденной аутентификации;

– сервисными билетами ST (*Service Tickets*), которые выдаются службой выдачи билетов TGS (*Ticket Granting Service*) и позволяют пользователю получить доступ к конкретному сервису приложений AS (Application Service).

При первичной аутентификации после успешного подтверждения подлинности пользователя KDC выдает первичное удостоверение пользователя для доступа к сетевым ресурсам – TGT. В последующем, пользователь при обращении к ресурсам сети предъявляет TGT и получает от KDC удостоверение для доступа к требуемому сетевому ресурсу – TGS.

При описании работы Kerberos используются следующие термины:

Клиент (*Client*) – сущность в сети (пользователь, сервис или хост), которая может получить билет от Kerberos.

Центр распределения ключей KDC (*Key Distribution Center*) – сервис, выдающий билеты Kerberos. В базе данных KDC вместе с информацией о каждом пользователе сохраняется криптографический ключ, известный только клиенту и службе KDC. Этот ключ создается на основе пароля пользователя и называется долговременным. Он используется для связи пользователя системы безопасности с центром распределения ключей.

Область (Realm) – совокупность серверов приложений и пользователей, информацию о которых имеет центр распределения ключей KDC. Для подсоединения пользователя в Realm у сервера аутентификации (Authentication Server) области Realm должны быть сведения об удостоверяющих данных этого пользователя, хранящиеся в защищённой базе данных безопасности Kerberos. Имя Realm совпадает с именем домена и обычно пишется в верхнем регистре, т. к. регистрозависимо.

В терминологии Kerberos домену соответствует область, которая обозначается заглавными буквами. Для домена astra.vas это будет область ASTRA.VAS.

Принципал (*Principal*) – учетная запись Kerberos с соответствующим набором прав, которая приблизительно соответствует термину «пользователь» и для которой разрешается аутентификация в Kerberos. Этот пользователь может получать разные наборы прав от Kerberos, что соответствует разным принципалам.

Принципал может быть:

– именем сервиса, который выполняется на хосте и называется принципалом сервиса (*Service-Principal*);

– именем пользователя, который называется принципалом пользователя (*User-Principal*).

Для информации об объекте, хранящейся в центре распределения ключей KDC (базе данных безопасности Kerberos), принципалы формируют индексное поле. Для сервисов и пользователей форматы принципалов различаются.

Имя принципала пользователя приблизительно соответствует имени учётной записи или имени пользователя и имеет форму principal-name[/instance-name]@REALM. Например, если имя пользователя в принципале пользователя – alice, а Realm – ASTRA.VAS, то полное имя принципала будет alice@ASTRA.VAS. Расширение instance-name позволяет иметь более одного принципала любому пользователю. Например, если alice является администратором области ASTRA.VAS, то alice/admin@ASTRA.VAS - имя её принципала, у которого будут другие удостоверяющие данные и права.

Принципал сервиса имеет форму service-name/QDN@REALM, где QDN – доменное имя хоста, на котором работает сервис, а service-name – строка, которая идентифицирует сервис на этом хосте (host). Например, для сервиса ftp, который работает на хосте с именем server.astra.vas в области ASTRA.VAS, имя принципала сервиса будет ftp/server.astra.vas@ASTRA.VAS.

Файлы ключей (*Keytab Files*) – файлы, которые содержат ключ шифрования для хоста или сервиса. Они извлечены из базы учетных записей KDC.

Суть Kerberos состоит в том, что область содержит как минимум один центр распределения ключей KDC (для обеспечения безотказности лучше больше), содержащий базу данных учетных записей. Если пользователь заходит на рабочую станцию под учетной записью, настроенной на Kerberos аутентификацию, KDC выпускает билет на получение разрешения TGT. Пользователь считается аутентифицированным, если он предоставляет совпадающие параметры, и тогда он может запрашивать сервисные билеты для сервисов, поддерживающих Kerberos, которые позволяют пользователю аутентифицироваться на сервисах без ввода имени и пароля, на сервере выдачи билетов (TGS).

Сервис Kerberos устанавливают в сети, в которой настроена служба доменных имен DNS. Каждому серверу, входящему в область Kerberos, должно быть присвоено полное квалифицированное доменное имя FQDN (*Fully Qualified Domain Name*), т. к. область Kerberos по соглашению совпадает с именем домена. Настроенный сервис DNS должен обеспечивать прямое и обратное разрешение FQDN. Чтобы отключить реверсивное разрешение, в файле конфигурации клиента krb5.conf нужно переменной rdns установить значение false.

Kerberos – зависимый от времени протокол, поэтому рабочая станция не будет аутентифицирована, если локальное время системы на сервере и на клиентской машине отличается более чем на 5 минут (по умолчанию). Простой и стандартный путь обеспечения синхронизации – использование сервиса NTP (*Network Time Protocol*).

Kerberos для контроля доступа к администрированию сервиса использует списки управления доступом ACL (Access Control List) [2, 3], которые позволяют настроить учетные записи и с более ограниченными правами. Списки находятся в файле /etc/krb5kdc/kadm5.acl.

Для обеспечения возможности авторизации пользователей через Kerberos используются подключаемые модули аутентификации в стеке авторизации PAM (*Pluggable Authentication Modules*),которые помогут выполнить аутентификацию в Kerberos в приложениях, использующих системную аутентификацию (например, login), а также при входе в систему. Для этого нужно подключить модули PAM, а для более тонкой их настройки отредактировать файл /etc/pam.d/common-auth. Механизм PAM, состоящий из набора разделяемых библиотек и конфигурационных файлов (сценариев процедур аутентификации), предоставляет единые механизмы для использования прикладных программ в процессе аутентификации и позволяет интегрировать различные низкоуровневые методы аутентификации.

В отличие от большинства служб аутентификации, в которых для защиты информации применяются асимметричные ключи, вся информация в Kerberos защищается с использованием симметричных ключей, но

несмотря на это принцип работы Kerberos напоминает инфраструктуру с частным открытым ключом.

Kerberos реализует систему многократного шифрования при передаче любой управляющей информации для избежания несанкционированного использования и перехвата информации. Только при условии достижения конфиденциальности и целостности транспортируемой управляющей информации, такая модель взаимодействия сервера и клиента может работать.

Список используемых источников

1. Буренин П. В., Девянин П. Н. и др. Безопасность операционной системы специального назначения Astra Linux Special Edition. Учебное пособие. Под редакцией доктора технических наук П. Н. Девянина. М.: Горячая линия – Телеком, 2018. 311 с.

2. Гринь Д. В., Ильина О. Б., Купчиненко О. П., Скоропад А. В. Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения Astra Linux SE // Региональная информатика и информационная безопасность: сб. тр. СПб.: СПОИСУ, 2017. Вып. 4. С. 76–78.

3. Ильина О. Б., Купчиненко О. П., Скоропад А. В. О механизмах дискреционного разграничения доступа в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2018. Т. 2. С. 356–360.

УДК 004.094:621.396.96
ГРНТИ 28.17.33

КОМПЛЕКС АЛГОРИТМОВ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ ПОДВИЖНЫХ ИСТОЧНИКОВ РАДИОСИГНАЛОВ НА ОСНОВЕ МЕТОДОВ ПРОГНОЗИРОВАНИЯ

С. С. Козин, Д. О. Маркин

Академия Федеральной службы охраны Российской Федерации

В статье приводятся основные результаты исследований по повышению эффективности позиционирования источников радиосигналов. Представлены результаты ряда экспериментов, в том числе натурных, позволяющих использовать в качестве исходных данных реальное распределение статистики уровня мощности принимаемого сигнала сотовой сети стандарта LTE, а также экспериментов, направленных на исследование эффективности математического аппарата нечеткой логики в совокупности с прогнозированием.

системы позиционирования, беспроводные сети передачи данных, трилатерация, нечёткая логика.

Современный уровень развития инфотелекоммуникационных технологий предоставляют все больше возможностей по доступу к услугам и данным с использованием беспроводных сетей передачи данных (БСПД). Вместе с тем возникает и угроза использования данных сетей в незаконных целях, связанных с распространением запрещенных сведений, несанкционированным доступом к защищаемой информации, сбором сведений о гражданах и организациях и других. Данное обстоятельство обуславливает объективную потребность в решении задачи оперативного определения местоположения (позиционирования) вероятного источника угрозы нарушения безопасности, в первую очередь, средствами самой беспроводной сети передачи данных.

Исследованиям вопросов использования БСПД в целях позиционирования источников радиоизлучения посвящены многочисленные исследования как отечественных, так и зарубежных ученых. Применение аппарата нечеткой логики для решения задачи позиционирования описано в трудах [1, 2]. Вопросами имитационного моделирования систем позиционирования посвящены работы Фокина Г. А. [3], Камалова Ю. Б. [4].

Вместе с тем, точность современных систем позиционирования в совокупности с их сложностью, предъявляют повышенные требования системам определения местоположения, которые в достаточной степени пока не удовлетворены.

Комплекс алгоритмов определения местоположения подвижных источников радиосигналов на основе методов прогнозирования

Для разработки имитационной модели необходимо разработать алгоритмы, осуществляющие моделирование следующих процессов:

– моделирование псевдослучайного движения подвижного источника радиосигналов по территории города;

– моделирование скорости и ускорения подвижного источника радиосигналов по территории города;

– моделирование псевдослучайного процесса распространения радиосигналов в условиях города.

Для осуществления данных функций выбрана платформа имитационного моделирования AnyLogic. Схема модели представлена на рис. 1.

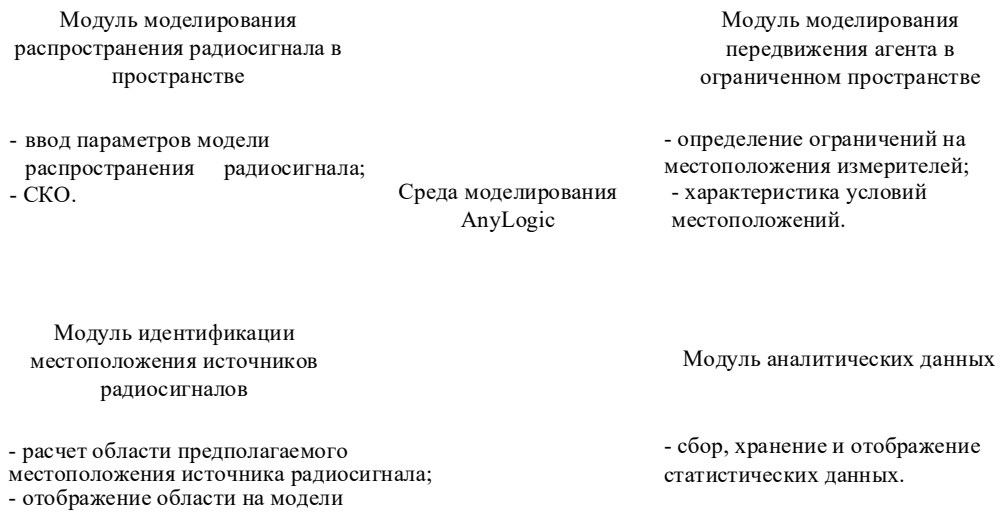


Рис. 1. Схема имитационной модели в среде AnyLogic

Для моделирования распространения радиосигналов в пространстве используется формула потерь для идеальной изотропной антенны.

Применение технологий трилатерации и нечеткой логики для решения задач позиционирования подробно описаны в работах [5, 6].

Реализация метода трилатерации в разрабатываемой системе представлена на рис. 2.

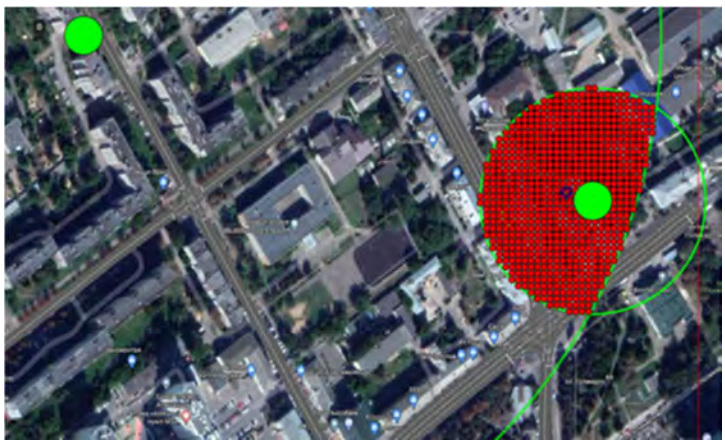


Рис. 2. Работа алгоритма трилатерации в разрабатываемой системе

Математический аппарат, позволяющий учитывать погрешность в расчётах, реализован в нечёткой логике. Для поиска местоположения на основе нечеткой логики используется накопленная статистика с данными о максимальной и минимальной ошибке позиционирования. Благодаря такому подходу, зона предполагаемого местонахождения объекта из круга уменьшается до кольца (в двумерной плоскости). Демонстрация данного эффекта и работа данного метода в разрабатываемой системе показаны на рис. 3.

Рис. 3. Работа алгоритма нечёткой логики в разрабатываемой системе

Эвристический метод позиционирования

Для определения более точного местоположения, необходимо произвести несколько расчетов, так как при большем количестве измерений, площадь поиска потенциального местоположения подвижного источника радиоизлучения уменьшается. При работе двух базовых станций возникают ситуации, когда областей возможного нахождения подвижного объекта две. Для устранения таких погрешностей был разработан эвристический алгоритм позиционирования на основе разбиения области возможного местонахождения объекта. Реализация данного алгоритма представлена на рис. 4.

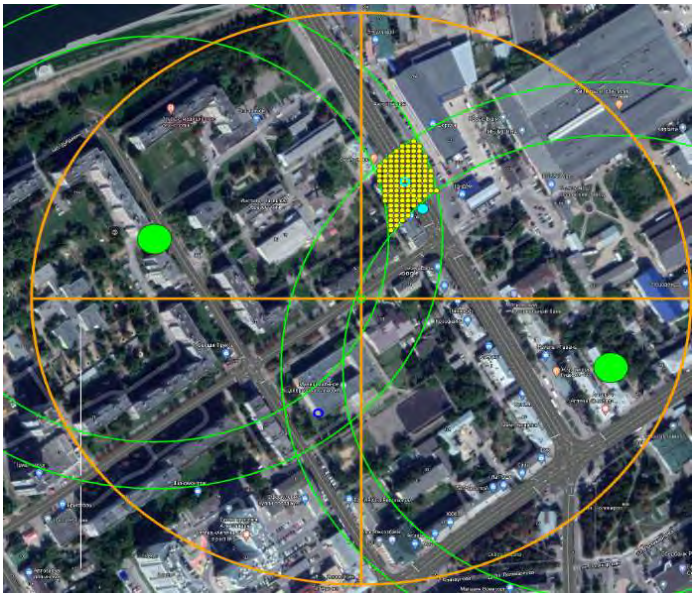


Рис. 4. Работа эвристического алгоритма позиционирования
в разрабатываемой системе

Оценка эффективности

Для оценки эффективности методов и алгоритмов в разработанной системе определения местоположения подвижного источника радиосигналов был проведён ряд экспериментов при работе различного числа БС и различных алгоритмах определения местоположения.

Основными параметрами, относительно которых производится расчет эффективности разработанного прототипа программного средства, являются площадь области предполагаемого местоположения объекта наблюдения, рассчитанная на основе метода Монте-Карло, а также расстояние от самого объекта до прогнозируемой, при помощи различных алгоритмов, точки.

Среднее число экспериментов для каждого из рассматриваемых случаев различно, и выбирается таким образом, чтобы именно при таком количестве испытаний процесс изменения параметров был наиболее приближен к эргодическому. Результаты эксперимента сведены в таблице 1 и 2.

ТАБЛИЦА 1. Среднее значение площади возможного местоположения подвижного источника радиосигналов

Алгоритм / Кол-во БС	Трилатерация, $м^2$	Нечёткая логика, $м^2$	Эвристический алгоритм прогнозирования, $м^2$
Одна БС	7 859,7	2 092	2 092
Две БС	1 343,5	247	131,6
Три БС	386	33	16

ТАБЛИЦА 2. Среднее значение расстояния от прогнозируемой точки до подвижного источника радиосигналов

Алгоритм / Кол-во БС	Трилатерация, м	Нечёткая логика, м	Эвристический алгоритм прогнозирования, м
Одна БС	487,5	487,5	487,5
Две БС	286	270,7	11,2
Три БС	133	8,74	3,52

Из таблиц, представленных выше, видно, что наиболее точные результаты по двум рассматриваемым критериям эффективности разрабатываемой системы даёт использование эвристического алгоритма позиционирования. В свою очередь, метод трилатерации даёт наименее точные результаты по сравнению с другими алгоритмами рассматриваемой си-

стемы определения местоположения подвижных источников радиоизлучения, связано это с простотой реализации данного алгоритма по сравнению с другими предложенными.

Выводы

В работе реализован комплекс моделирующих алгоритмов, реализующих ряд случайных процессов, таких как движение подвижных источников радиосигналов и распространение радиоволн, а также алгоритмы, осуществляющие аналитический расчет предполагаемой области местоположения на основе аппарата нечеткой логики, а также методов прогнозирования: линейное предсказание и эвристический алгоритм прогнозирования на основе секторного разбиения областей; получена сравнительная оценка эффективности алгоритмов определения местоположения подвижных источников радиосигналов.

Экспериментально проверена и подтверждена работоспособность данной системы определения местоположения подвижных источников радиосигналов. Программные реализации методов, реализованные в данной системе, зарегистрированы в ФИПС [7, 8].

Список используемых источников

1. Socha, Michał; Górka, Wojciech; Kostorz, Iwona. Fuzzy logic in indoor position determination system // Theoretical and Applied Informatics. 2016. Vol. 27. Pp. 1–15.

2. Orujov, F.; Maskeli, R.; Damaševičius, R.; Wei, Wei; Ye Li Smartphone based intelligent indoor positioning using fuzzy logic // Future Generation Computer Systems. 2018. No. 89. Pp. 335–348.

3. Фокин Г. А. Технологии сетевого позиционирования 5G: монография. СПб.: СПбГУТ, 2020. 466 с.

4. Камалов Ю. Ю., Служивый М. Н. Имитационное моделирования мобильных систем связи в условиях городской застройки // Известия Самарского научного центра РАН. 2010. Т. 12, № 4 (2). С. 341–345.

5. Вишнякова О. А., Лавров Д. Н., Лаврова С. Ю. Математическая модель обнаружения точки беспроводного доступа по измерениям мощности излучения разнесенными наблюдателями // Математические структуры и моделирование / Ом. гос. ун-т. Фак. компьютер. наук. Омск : Изд-во ОмГУ. 2013. № 2 (28). С. 49–59.

6. Маркин Д. О. Исследование эффективности алгоритмов определения местоположения мобильных устройств внутри помещений // Вестник РГРТУ. 2015. № 54-1. С. 32–39.

7. Программное средство определения местоположения подвижных источников радиосигналов на основе методов прогнозирования : свидетельство о государственной регистрации программы для ЭВМ № 2020666496 Российская Федерация / С. С. Козин, А. А. Кузькин, Д. О. Маркин, В. В. Рябоконь, Д. А. Свечников, О. А. Субботенко; авторы и правообладатели С. С. Козин, А. А. Кузькин, Д. О. Маркин, В. В. Рябоконь, Д. А. Свечников, О. А. Субботенко. – № 2020665135 ; заявл. 24.11.2020; опубл. 10.12.2020; зарегистрировано в Реестре программ для ЭВМ 10.12.2020 г.

8. Средство идентификации нелегитимных неподвижных источников радиосигналов беспроводных сетей передачи данных : свидетельство о государственной регистрации программы для ЭВМ № 2020611627 Российская Федерация / Д. О. Маркин, С. С. Козин, М. К. Бирюков, Т. А. Кравчук, В. А. Сидорова ; авторы и правообладатели Д. О. Маркин, С. С. Козин, М. К. Бирюков, Т. А. Кравчук, В. А. Сидорова. – № 2020615423 ; заявл. 01.06.2020; зарегистрировано в Реестре программ для ЭВМ 11.06.2020 г.

УДК 004.4'27
ГРНТИ 50.41.25

ПРОЦЕСС СОЗДАНИЯ 3D ПЕРСОНАЖА И СПОСОБЫ АВТОМАТИЗАЦИИ ЕГО ЭТАПОВ

Н. А. Колосков, А. В. Фёдорова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена процессу создания 3D персонажа для дальнейшего использования в разработке игр. Приводится описание конвейера разработки 3D модели. С помощью иллюстраций наглядно показываются некоторые этапы разработки. Приводятся примеры автоматизации этапов, их преимущества и недостатки. По обзору, приведенному в статье, делаются выводы о текущем состоянии дел в рассматриваемой области и о перспективах ее развития.

3D, игровые модели, скульптурирование, ретопология.

Компьютерная графика используется во многих областях промышленности, но самое актуальное место занимает в игровой индустрии. Многие программы для компьютерной 3D графики в первую очередь ориентируются на игровую индустрию. Сам процесс создания моделей называется конвейер (*pipeline*) и имеет собственные этапы. В него входят: подготовка идеи и концепции, скульптурирование высоко полигональной (*high-poly*) модели, ретопология, развертка, текстурирование, анимация (рис. 1).

Также существуют способы автоматизации этих этапов, благодаря чему можно сократить время на создание модели и сэкономить ресурсы на производстве графики.

Отправной точкой почти каждой модели является концепт, идея или референс, который используется для создания чистого и понятного визуального образа модели. В процессе отбора разных источников необходимо подобрать правильные референсы, так как это поможет в дальнейшем больше не обращаться к поиску источников и на последних этапах не затруднит работу с полностью готовой моделью.

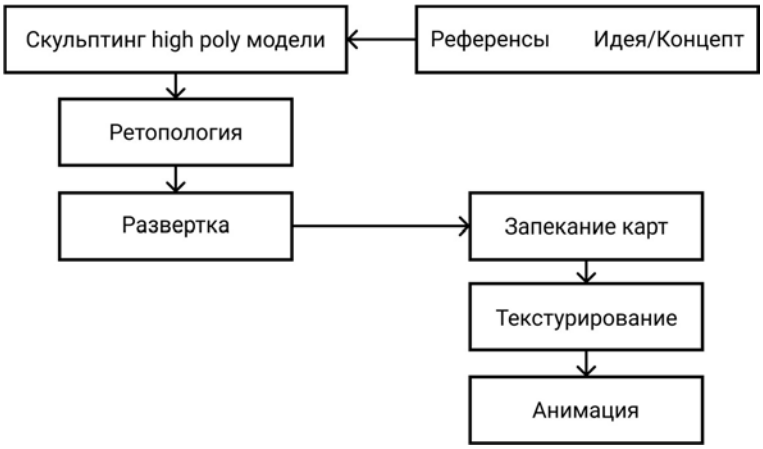


Рис. 1. Конвейер создания 3D моделей

Далее следует этап скульптурирования. Один из самых объемных по работе. В процессе выполнения этого этапа разными способами создается низко полигональная модель. Полигон – это минимальная поверхность, из которой складываются каркасы форм любой сложности [1]. Разные модели требуют разного количества полигонов, но для того, чтобы добиться реалистичности требуется большее количество полигонов. Их количество может доходить до нескольких десятков миллионов, что в свою очередь влияет на потребляемые ресурсы компьютером для обсчета каждой модели.

Для дальнейшей работы с моделью требуется уменьшить количество полигонов до нескольких тысяч. Это этап ретопологии, в процессе которой теряется мелкая детализация объекта, пример на рис. 2.

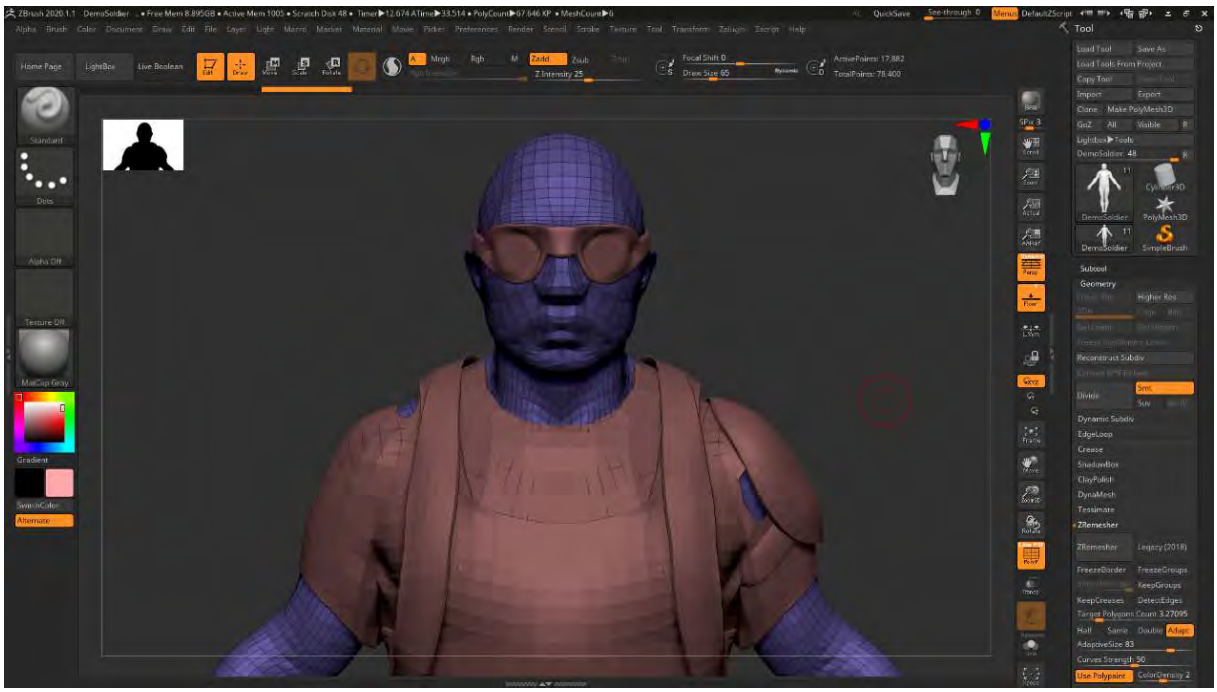


Рис. 2. Автоматическая ретопология модели Zremesher до 17 882 полигонов

В его процессе создается низко полигональная модель разными способами. Вручную этот процесс занимает до нескольких часов, но его можно автоматизировать с помощью встроенных программных средств в Zbrush, или же Instant meshes remesher. Программы с помощью внутренних алгоритмов самостоятельно уменьшают количество полигонов, но в таком методе есть свои минусы. Алгоритмы не разделяют важные и неважные участки, например лицо модели и спина будут одинаково восприниматься алгоритмами и в таком случае детализация лица может пострадать, а вот количество полигонов на относительно ровной спине может превышать нужное количество. Поэтому в зависимости от каждой модели нужно выбирать подходящий метод.

Этап создания развертки модели позволяет разложить объемную модель на 2d «карту», пример на рис. 3, он нужен для дальнейшего текстурирования и правильного отображения текстур на модели. Этот этап максимально автоматизирован в современных программах.

Этап текстурирования включает в себя несколько подэтапов. Сначала идет процесс запекания карт нормалей (*normal map*) и карт смещения (*displacement map*) [2, 3]. С помощью карт нормалей можно перенести детализацию с высоко полигональной модели на низко полигональную после процесса ретопологии. Карта нормалей изменяет отражение света, и позволяет сымитировать сложную поверхность не повышая количество полигонов. Карта смещения уже не имитируют сложную поверхность, а они ее создают на модели, что в свою очередь замедляет процесс отображения модели. Дальше можно текстурировать саму модель, то есть наносить нужные цвета и текстуры на определенные участки модели или целиком на всю.

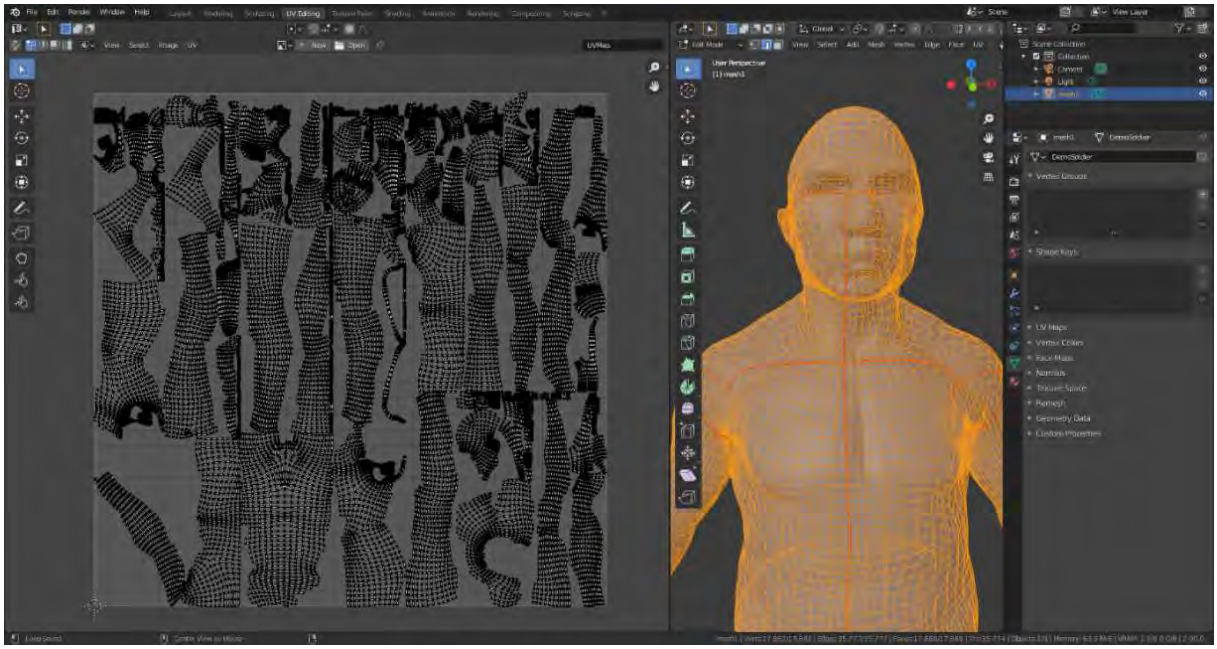


Рис. 3. Развертка 3D модели

Последний этап анимации включает в себя создание скелета модели и привязки его к самой модели. Скелетом он называется условно, хотя у всех подвижных частей создаются «кости», с помощью которых будет анимироваться в дальнейшем. Во время привязки скелета к модели, всем вершинам полигонов, вертексам, присваивается свой «вес». В зависимости от его величины в программе правильно сгибаются конечности без искажений. На этом этапе можно применить программу Cascadeur для создания анимации персонажа с помощью алгоритмов программы. Cascadeur – программа для создания ключевой анимации 3D персонажей (гуманоидных и не только) [4]. Программа довольно точно определяет скелет модели и может анимировать физически корректно. Что в свою очередь уменьшает количество работы над анимацией.

В результате обзора, выполненного в статье, можно сделать следующие выводы о текущем состоянии дел в рассматриваемой области и о перспективах ее развития:

1) Прохождение всех этапов разработки модели позволяет использовать ее в конечной игре как готовый программный продукт.

2) Использование способов автоматизации при разработке модели позволяет сэкономить время и ресурсы.

3) Способов автоматизации в рассматриваемой области на сегодняшний день существует ограниченное количество.

4) Развитие соответствующих технологий стимулирует к разработке новых методов автоматизации процесса создания 3D моделей.

5) Разработка новых методов автоматизации процесса создания 3D моделей является областью, требующей соответствующих научных исследований и перспективным практическим направлением разработок.

Список используемых источников

1. Бердичевский Е. Г. Полигональная графика как инструмент трехмерного моделирования // Геометрия многообразии и ее приложения: Материалы Пятой научной конференции с международным участием, посвященной 100-летию профессора Р. Н. Щербакова. Улан-Удэ: Бурятский государственный университет имени Доржи Банзарова, 2018. С. 79–86.

2. Это норма: что такое карты нормалей и как они работают. URL: https://habr.com/ru/post/481480 (дата обращения 10.03.2021).

3. В чем разница между bump, normal и displacement? URL: https://3dpapa.ru/v-chem-raznica-mezhdu-kartami-bump-normal-i-displacement (дата обращения 10.03.2021).

4. Программа для physics-based анимации 3D персонажей. URL:https://cascadeur.com/ (дата обращения 10.03.2021).

УДК 004.514
ГРНТИ 20.53.19

МЕТОДИКА «БЫСТРЫХ КОМАНД», КАК НОВЫЙ ОПЫТ ПРОСЛУШИВАНИЯ МУЗЫКАЛЬНЫХ КОМПОЗИЦИЙ

Т. В. Мусаева, П. О. Кольцов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье описывается роль быстрых команд в таком процессе, как прослушивание музыкальных композиций. Иногда упускаются из виду потенциальные инновации, которые могли бы улучшить наш опыт прослушивания музыки. Пользователи взаимодействуют с аудиоплеером с помощью стандартного набора кнопок – «слушать», «пауза», «перемотать назад», «перемотать вперёд» и т.д. Это вовсе не означает, что данный опыт взаимодействия достиг совершенства. В статье рассматривается понятие быстрых команд и то, каким образом их можно использовать для улучшения опыта взаимодействия с аудиоплеером.

быстрые команды, опыт прослушивания, аудиоплеер, пользовательский интерфейс, информационные системы.

Сегодня пользователям предлагается множество возможностей для прослушивания аудиоконтента – от сервисов потокового аудио до обычных цифровых аудиоплееров. Сервисы потокового аудио сегодня имеют наибольшую пользовательскую базу. По данным опубликованного исследовательской компанией Counterpoint Research отчёта состояние рынка сервисов потокового аудио в 2019 году следующее (рис. 1): Spotify имеет долю рынка 35 % (компания получает 31 % общего дохода отрасли), Apple Music имеет 19 % подписок и 24 % прибыли, Amazon Music – 15 %, Tencent Music – 11 %, YouTube Music – 6 % [1].

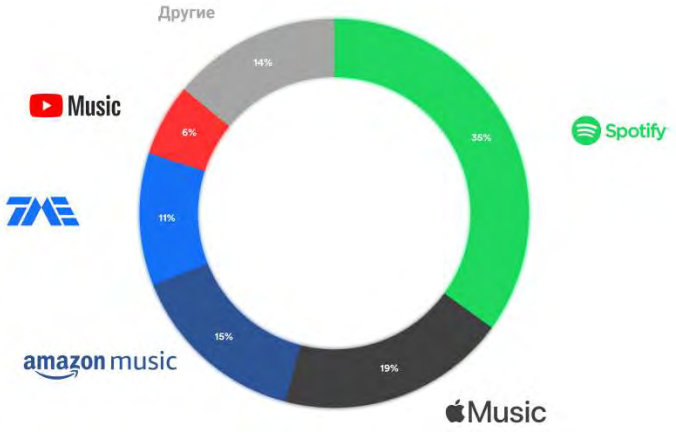


Рис. 1. Рынок сервисов потокового аудио

В компании Counterpoint Research утверждают, рост числа пользователей платных подписок обусловлен проведением сервисами рекламных акций со снижением цен и публикацией эксклюзивов. Эксперты ожидают, что показатель вырастет до 280 млн подписок к концу 2021 года.

В 2020 году крупнейшие сервисы потокового аудио объявили о партнёрстве с Musixmatch – компанией, которая предоставляет доступ к синхронизированным по времени текстам песен [2]. Такая возможность доступна для пользователей 26 стран. Партнерство привнесло в сервисы потокового аудио новые возможности, благодаря которым пользователи могли искать любимую музыку по фрагменту текста и подпевать [3].

Перечисленные возможности изменили процесс прослушивания музыки, сделали его более увлекательным. Однако эти возможности не полностью раскрывают потенциал сервисов.

Основная идея – внедрение «быстрых команд» для улучшения интерактивного взаимодействия с музыкальными композициями в стриминговых сервисах. У каждого аудиоплеера существует стандартный набор элементов управления, состоящий из кнопок – «воспроизведение/пауза», «перемотать вперёд», «перемотать назад» и «регулятор поиска». Но текущий набор элементов не позволяет осуществлять полный контроль над воспроизведением композиции. Иногда у пользователя возникает потребность продемонстрировать определённую часть песни, но из-за отсутствия необходимой навигации это становится непростой задачей. Пользователю приходится перемещать ползунок по временной шкале пальцем вперед или назад, глядя на быстро изменяющиеся значения времени до тех пор, пока не удастся найти необходимый фрагмент. Управление прогрессом в аудиоплеере происходит с помощью «регулятора поиска» (рис. 2).

Рис. 2. Элемент управления «регулятор поиска»

Элемент управления «регулятор поиска» имеет огромный потенциал для расширения исполняемых им функций. Введем понятие «быстрые команды» – теги, позволяющие помечать части текста музыкальной композиции. В структуре музыкальной композиции используются следующие теги: «вступление» (англ. *intro*), «куплет» (англ. *verse*), «предприпев» (англ. *pre-chorus*), «припев» (англ. *chorus*), «постприпев» (англ. *post-chorus*), «инструментал» (англ. *instrumental*), «бридж» (англ. *bridge*) и «концовка» (англ. *outro*). Стандартная структура музыкальной композиции представлена на рис. 3.

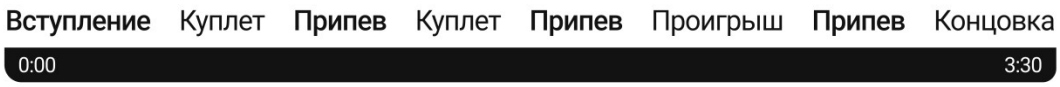


Рис. 3. Структура музыкальной композиции

С помощью «быстрых команд» пользователь на выделенном для решения данной задачи ресурсе сможет определить структуру песни (например, на уже существующем сервисе Musixmatch), а затем синхронизировать все строки по времени для дальнейшего интерактивного взаимодействия. «Быстрые команды» позволят пользователю во время прослушивания музыкальной композиции переходить к необходимому фрагменту песни с помощью специальной интерактивной панели, расположенной над «регулятором поиска». На рис. 4 представлен разработанный концепт интерфейса Spotify с данной функцией.

Внедрение представленной методики откроет пользователю новые возможности по быстрому обучению работы с интерфейсом, такие как интуитивное:

– восприятие ее структуры по правилу «понимаю, где и что находится, и что нужно делать дальше»;

– понимание содержательной части по правилу «изображение – метафора – текст»;

– навигация между ее составными частями по правилу «логическое путешествие по ссылкам, переходы и возврат домой».

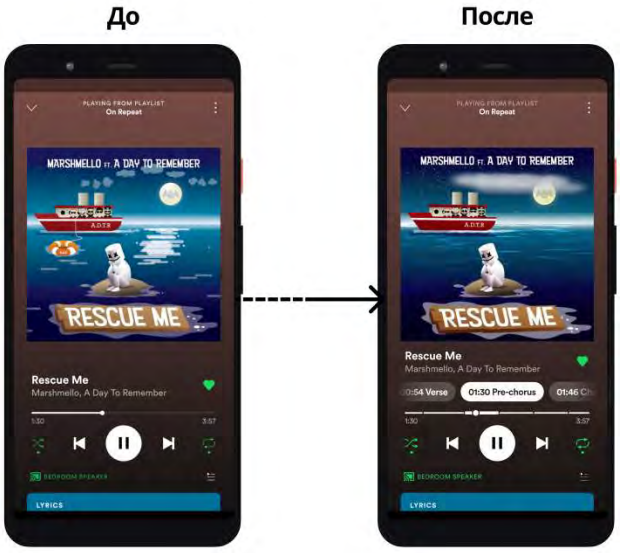


Рис. 4. Пользовательский интерфейс приложения (до и после внедрения функции)

Список используемых источников

1. Global Online Music Streaming Grew 32% YoY to Cross 350 Million Subscriptions in 2019 // Counterpoint Technology Market Research. URL: https://www.counterpoint-research.com/global-online-music-streaming-revenues-cross-us11-billion-h1-2019/ (дата обращения 10.02.2021).

2. What is Musixmatch // Medium. URL: https://blog.musixmatch.com/what-is-musixmatch-71c38e2a7b5d#.fr69hjhii (дата обращения 15.02.2021).

3. In a significant expansion, Spotify to launch real-time lyrics in 26 markets // TechCrunch. URL: https://techcrunch.com/2020/06/29/in-a-significant-expansion-spotify-to-launch-real-time-lyrics-in-26-markets/ (дата обращения 17.02.2021).

УДК 004.42
ГРНТИ 50.49.37

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ УЧЕТА ОБОРУДОВАНИЯ НА ПРЕДПРИЯТИИ

Н. В. Кривоносова, Н. Е. Терещенко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Учет оборудования на предприятии – один из обязательных бизнес-процессов. Существующие программные решения для автоматизации учета оборудования на сегодняшний день не всегда доступны по стоимости на закупку и эксплуатацию, а также не всегда в полной мере удовлетворяют требованиям компании.

информационная система, учет оборудования.

Актуальность задачи по автоматизации учета компьютерного и другого оборудования на предприятии возрастает при наличии значительного парка компьютеров, офисной техники и другого оборудования. Потребность в знании, где и какая единица располагается, в оперативном отслеживание изменений, связанных с оборудованием, возникает в основном у ИТ-подразделений. Особую значимость задача автоматизации учета оборудования приобретает на крупных предприятиях. Обработка постоянно растущих массивов информации возможна только с использованием современных компьютерных технологий. Организовать систему учёта техники на предприятии, вести учёт компьютеров и комплектующих сейчас невозможно без дополнительно установленного на компьютер программного обеспечения. (Кузнецов, 2007) [1].

Любая вычислительная или офисная техника определяется сроком службы, нуждается в ремонте, пересмотре, замене каких-либо деталей, обновлением и весь этот учёт, из-за большого количества компьютерной и офисной техники, трудно вести вручную, так как это занимает более длительное время и требует конкретного и точного внимания.

Информационная система по учету инфокоммуникационного оборудования предназначена для автоматизации процесса сбора и хранении информации о характеристиках компьютеров и периферийных устройств.

Хранение данных об оборудовании будет осуществляется в реляционной базе данных, размещённой на локальном сервере. Сервер будет использоваться от компании Microsoft. Система управления базой данных-MS Management Studio [1]. (Кузнецов) (Язык программирования C# и платформа .NET.) (Кузнецов, 2007) Программа будет взаимодействовать с сервером и базой данных, в частности, по средствам Entity Framework, так

как это наиболее технологичное и удобное средство взаимодействия на настоящее время. Программный продукт будет разрабатываться на языке C#, [2]так как он наиболее удобен для реализации поставленных задач. Проектировка базы данных и того, как различные модули будут взаимодействовать между собой, будет происходить в MS Visio.Внешняя составляющая программного продукта будет разрабатываться в Figma.

В базе данных будет хранится информация о типе оборудования, его серийный номер, инвентарный номер, дата поставки на предприятие, дата записи в базу, описание характеристики оборудования, а также отдел/помещение, в котором оно установлено [1].

Данные из базы данных будут выводится в сводную таблицу, удобную для восприятия. Для этой таблицы можно будет применять фильтры по любому из полей, а также сортировать в порядке возрастания или убывания.

В программе будет реализована возможность регистрации разных пользователей с правами обычного пользователя или администратора, добавлять в базу, изменять и удалять оборудование из базы данных [1].

Планируется также сделать вывод различных отчетов и статистики, а кроме этого, добавить фотоидентификацию оборудования [4].

База данных

Таблица Brand используется для записи наименований производителей, техника которых используется на предприятии. Поля таблицы:

- ID – номер записи(int);
- Title – наименование производителя (varchar (50)).

Таблица Equipment нужна для описания оборудования. Поля таблицы:

- ID – номер записи(int);
- TypeEqipmentID – номер типа оборудования, который подтягивается из таблицы TypeEquipment(int);
- Title – наименование оборудования (varchar (100));
- BrandID-ID производителя, подтягивается из таблицы Brand(int);
- Description –описание оборудования (varchar (2000)).

Таблица Place требуется для описания места, где расположено оборудование. Поля таблицы:

- ID – номер записи(int);
- Title – наименование места (кабинет, помещение, отдел) (varchar (50));
- Floor –этаж (varchar (10)).

Таблица Placement используется для куда и когда было перемещено оборудование. Поля таблицы:

- ID – номер записи(int);
- PlaceID – ID места размещение(int);
- MovingDate – дата перемещение(date).

Таблица Provider нужна для записи поставщиков оборудования. Поля таблицы:

- ID – номер записи(int);
- Title – наименование поставщика (varchar (50));
- PhysicalAddress – физический адрес (varchar (500));
- Phone – контактный телефон (varchar (50));
- Email – электронная почта (varchar (100)).

Таблица EquipmentType требуется для записи видов и типов оборудования. Поля таблицы:

- ID – номер записи(int);
- Title – вид оборудования (varchar (50));
- Type – тип оборудования(varchar(50)).

Таблица UsersType нужна для записи видов пользователей. Поля таблицы:

- ID – номер записи(int);
- Title – наименование вида(varchar(50)).

Таблица Users используется для записи пользователей системы. Поля таблицы:

- ID – номер записи(int);
- Surname – фамилия пользователя(varchar(20));
- Patronymic – отчество пользователя(varchar(20));
- Name – имя пользователя (varchar(20));
- DateOfBirth – дата рождения(date);
- Email – электронная почта(varchar(50));
- UserTypeID – код типа учетной записи, подтягивается из таблицы UserType(int);
- Password – пароль от учетной записи пользователя (varchar(50)).

Архитектура программного продукта

Архитектура типа клиент-сервер. В качестве сервера SQL Server Express наиболее подходит для текущей работы по начальной проработке информационной системы по следующей причине: размещается локально на компьютере и не требует покупки. Клиент представляет собой приложение, разработанное на языке WPF C#. Для связи проекта и сервера использована технология Entity Framework. (Язык программирования C# и платформа .NET., 2020) [4].

Бизнес-требования

Создание информационной системы по интерфейсу схожей с аналогичной существующей, но не имеющей недостатков последней.

Пользовательские требования [3].

Продукт должен предоставлять возможность просмотра всей информации по оборудованию.

Функциональные требования.

– возможность добавления, изменения и удаления информации по тому или иному оборудованию;

– возможность задания фильтрации и сортировки данных по определенным параметрам;

– возможность просмотра основной информации по оборудованию, такой как: наименование, тип, место размещения, описание комплектации, инвентарный номер, серийный номер, поставщик, дата поставки, дата установки, перемещения.

Нефункциональные требования.

– операционная система Windows 8 и выше;
– оперативная память должна быть не менее 2 гигабайт (Гб);
– объем свободного места на жестком диске 200 Мб;
– клавиатура и мышь (или совместимое устройство ввода).

Требования по стилю:
Шрифт: Times New Roman;
Цвет:
– для заголовков : RGB(115, 217, 249);
– фон: RGB(205, 236, 242) [3].

Список используемых источников

1. Кузнецов С. Д. Основы баз данных. 2-е изд. М.: Интернет-университет информационных технологий - ИНТУИТ.ру, 2007. 488 с. ISBN 978-5-94774-736-2

2. Скит, Джон. C# для профессионалов. Пер. с англ. М. : ООО. “И.Д. Вильямс”, 2014. 608 с. : ил.

3. Мартин, Роберт Сесил. Чистый код. СПб.: Питер, 2019. 465 с.

4. METANIT.COM: сайт о программировании. URL: https://metanit.com/sharp/.

Работа представлена директором СПбКТ Т. Н. Сиротской.

УДК 02.026 (681.3)
ГРНТИ 20.53.01

ОБОСНОВАНИЕ ЭТАПОВ МЕТОДА ИНТЕРВАЛЬНОГО ОЦЕНИВАНИЯ КАЧЕСТВА ЭЛЕКТРОННЫХ БИБЛИОТЕК

Е. С. Крюкова, И. Б. Паращук

Военная академия связи

Рассматриваются вопросы анализа сущности и содержания этапов метода интервального оценивания качества функционирования современных электронных библиотек. Анализируются последовательность реализации этих этапов, их функции и задачи. Исследование проводилось с целью систематизации и выявления особенностей определения интервальных (нижней и верхней) оценок качества электронных библиотек на основе методов теории интервальных средних в интересах достоверного анализа и повышения качества управления структурой, параметрами и режимами работы систем такого класса.

электронная библиотека, показатель, качество, интервальные средние, оценивание, метод, этапы.

Современные электронные библиотеки (ЭБ) по праву относятся к классу сложных управляемых информационных систем [1, 2, 3]. Традиционные методы, составляющие методологию оценивания состояния, качества и эффективности таких сложных информационных систем и ориентированные на использование обобщенных (комплексных) показателей качества [4, 5], связаны с интегрированием (по пороговым значениям параметров и показателей качества систем такого класса) совместных плотностей распределения вероятностей, описывающих эти показатели качества.

Известно, что такие текущие совместные плотности распределения вероятностей имеют размерность $K \times M \times T$, где K – число ПК системы (например, ЭБ), M – число состояний этих ПК ЭБ, а T – число временных отсчетов анализа ПК ЭБ. Этот факт указывает на необходимость при оценивании обобщенных (комплексных) показателей качества ЭБ использовать процедуры непосредственного K-кратного интегрирования совместной плотности распределения вероятностей размерности $K \times M \times T$, что приводит к явлению, называемому в математике «проклятием размерности».

С этой точки зрения, предлагаемые и исследуемые подходы к интервальному оцениванию качества, рассматриваемые нами показатели качества (ПК) ЭБ и параметры процесса их функционирования на определенном временном интервале, имеют очевидные преимущества.

Предлагаемая совокупность методов оптимального оценивания частных показателей качества функционирования ЭБ на определенном временном интервале, основанная на методах теории интервальных средних и методах теории фильтрации, позволяет, в отличие от общепринятых комплексных методов, значительно сократить размерность задачи оценивания, предполагая наличие двухэтапной процедуры:

I этап – применение модели смены состояний ПК ЭБ в виде непрерывных цепей Маркова в форме разностных стохастических уравнений, что позволяет свести размерность задачи к $K \times M \times \tau$, где τ – временные интервалы оценивания ПК ЭБ [6];

II этап – замена процедуры непосредственного K-кратного интегрирования совместной плотности распределения вероятностей размерности $K \times M \times \tau$ процедурами сбора данных наблюдения (или моделирования) и вычисления оценочных значений нижнего и верхнего средних уровней качества (частных ПК) элементов ЭБ и ЭБ в целом на интервале времени $(\tau + \Delta\tau)$ с использованием методов теории интервальных средних.

Таким образом, предлагаемые методы интервального оценивания частных показателей качества функционирования ЭБ на определенном временном интервале, основанные на постулатах теории интервальных средних и алгоритмах оптимальной фильтрации (экстраполяции), позволяют осуществить переход к текущей пошаговой фильтрации ПК ЭБ и к получению оценочных значений нижнего и верхнего средних уровней качества (частных ПК) ЭБ на интервале времени $(\tau + \Delta\tau)$ с использованием методов теории интервальных средних. При этом временной интервал оценивания $(\tau + \Delta\tau)$ включает конечное множество T непрерывных отсчетов наблюдения (моделирования): $(\tau + \Delta\tau) = \{(t_1 + \Delta t) + (t_2 + \Delta t) + \ldots + (t_T + \Delta t)\}$.

Ключевыми этапами интервального оценивания частных показателей качества функционирования ЭБ являются:

Сбор (с использованием математической, имитационной модели или на основе наблюдения в реальной ЭБ) статистических данных о значениях ПК ЭБ $\vec{X}_j(t + \Delta t) = f(x_1(t + \Delta t); x_2(t + \Delta t); \ldots x_i(t + \Delta t); \ldots x_N(t + \Delta t))$ за период наблюдения или шаг моделирования (на $(t + \Delta t)$-ом временном отрезке функционирования ЭБ).

Оптимальная по критерию минимального среднего квадрата ошибки (МСКО) фильтрация значений показателей качества электронных библиотек $\hat{\vec{X}}_j(t + \Delta t) = f(\hat{x}_1(t + \Delta t); \hat{x}_2(t + \Delta t); \ldots \hat{x}_i(t + \Delta t); \ldots \hat{x}_N(t + \Delta t))$ за период наблюдения или шаг моделирования (на $(t + \Delta t)$-ом временном отрезке функционирования ЭБ).

Формирование интервального оценочного нижнего $\underline{\hat{x}_i}(\tau + \Delta\tau)$ и верхнего $\overline{\hat{x}_i}(\tau + \Delta\tau)$ средних уровней значений каждого из ПК ЭБ на интервале времени

оценивания ($\tau + \Delta\tau$) на основе оценочных значений этих ПК за все непрерывные отсчеты (периоды) наблюдения или шаги моделирования ($t + \Delta t$), составляющие в сумме содержание шага оценивания ($\tau + \Delta\tau$).

Определение интервальных оценок нижних $\underline{\hat{\bar{X}}}(\tau+\Delta\tau)$ и верхних $\overline{\hat{\bar{X}}}(\tau+\Delta\tau)$ значений обобщенного показателя (коэффициента) качества ЭБ с учетом результатов интервальных оценок (идентификации) ее частных ПК.

Взаимосвязь перечисленных этапов и влияющих факторов представлена на рис.

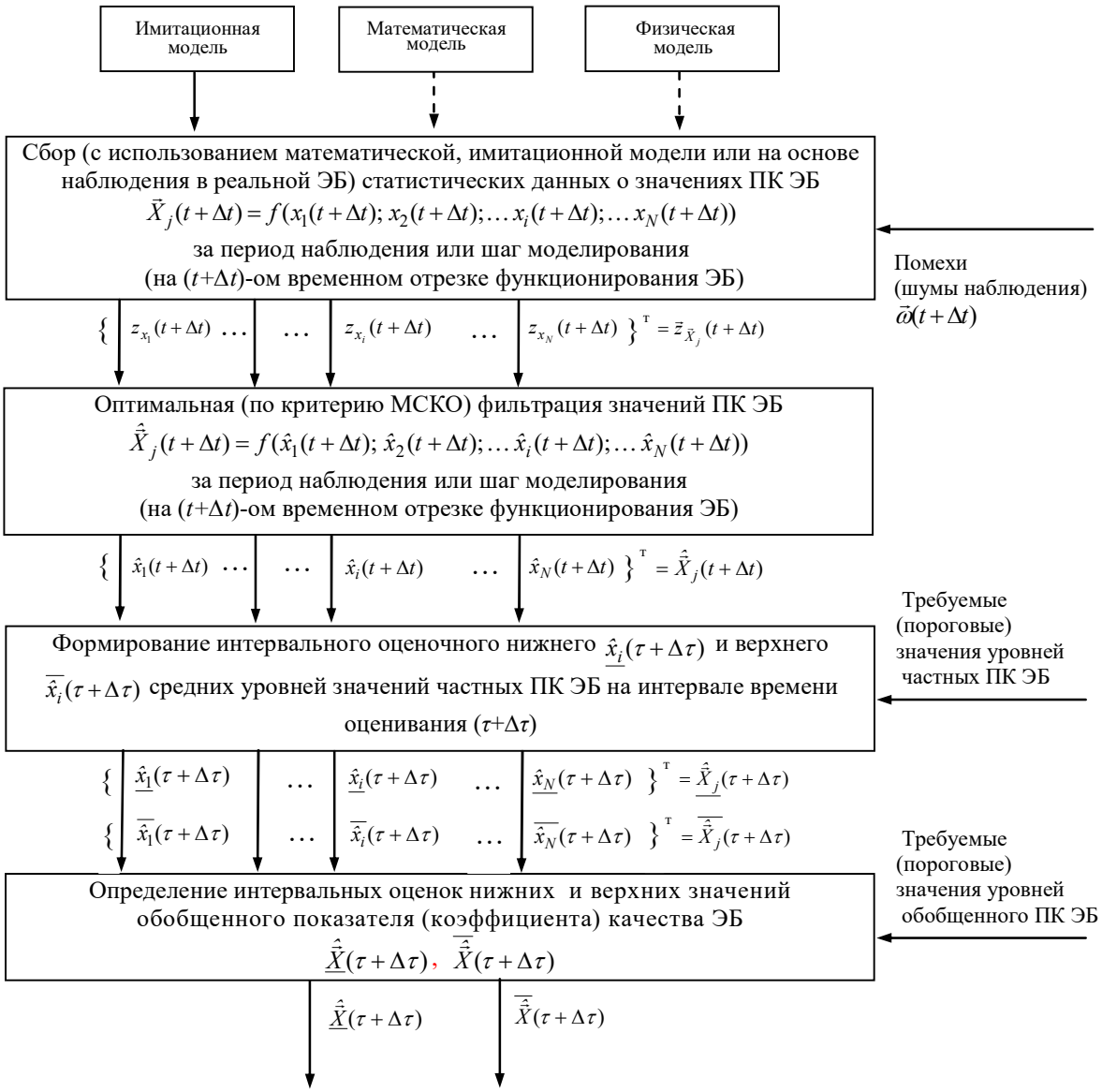


Рис. Этапы метода интервального оценивания качества функционирования электронных библиотек

Таким образом, в рамках рассмотренных этапов (см. рис. 1), на основе статистического анализа измеряемых (наблюдаемых, моделируемых) параметров и с использованием методов теории интервальных средних находят нижний и верхний средние уровни качества элементов ЭБ и ЭБ в целом на интервале времени ($\tau + \Delta\tau$). Рассчитывается точное нижнее $\underline{\hat{x}_i}(\tau+\Delta\tau)$ и верхнее $\overline{\hat{x}_i}(\tau+\Delta\tau)$ значение среднего уровня частных показателей качества ЭБ, наблюдаемых на интервале времени оценивания ($\tau+\Delta\tau$), путем решения задачи линейного программирования на основе средних значений идентифицированных параметров системы [7].

Важен как предпоследний, так и заключительный этап – определение интервальных оценок обобщенного показателя (коэффициента) качества ЭБ с учетом результатов интервального анализа (идентификации) параметров системы. При этом при анализе качества не используется информация о независимости элементов ЭБ. В этих условиях для систем с мультипликативным обобщенным показателем (коэффициентом) качества, используется соотношение, характеризующее функцию взаимосвязи обобщенных показателей (коэффициентов) качества ЭБ с частными *j*-ми ($j = 1, \ldots, J$) показателями качества:

$$\underline{\hat{\hat{X}}}(\tau+\Delta\tau) = \prod_{j}^{J} \underline{\hat{\hat{X}}_j}(\tau+\Delta\tau);$$

$$\overline{\hat{\hat{X}}}(\tau+\Delta\tau) = \min_{j=1,\ldots,J} \overline{\hat{\hat{X}}_j}(\tau+\Delta\tau).$$

Таким образом, могут быть получены интервальные частные (нижняя и верхняя) оценки качества и обобщенная оценка качества ЭБ на основе методов теории интервальных средних. Полученные интервальные результаты контроля, оценочные значения параметров системы за интервал времени, позволят повысить достоверность оценивания качества ЭБ, что, в конечном итоге, сыграет свою важную роль в повышении качества управления структурой, параметрами и режимами работы систем такого класса.

Список используемых источников

1. Зуйкина К. Л., Соколова Д. В., Скалабан А. В. Электронные библиотеки в России. Текущий статус и перспективы развития. М.: Ваш формат, 2017. 120 с.

2. Антопольский А. Б., Маркарова Т. С., Крюкова О. П., Харламов А. А. Электронные библиотеки в образовании / Под редакцией О. П. Крюковой, А. А. Харламова. М.: 2009. 94 с.

3. Национальный стандарт Российской Федерации ГОСТ Р 7.0.96 - 2016. Электронные библиотеки. Основные виды. Структура. Технология формирования. М.: Стандартинформ, 2016. 13 с.

4. Петухов Г. Б. Основы теории эффективности целенаправленных процессов. М.: МО СССР, 1989. 660 с.

5. Терентьев В. М., Паращук И. Б. Теоретические основы управления сетями многоканальной радиосвязи. СПб.: ВАС, 1995. 195 с.

6. Крюкова Е. С. Модель функционирования электронной библиотеки для анализа ее качества и информационной безопасности // Вопросы оборонной техники. Научно-технический журнал. Технические средства противодействия терроризму. Серия 16. Выпуск № 9-10 (147-148), 2020. С. 16–22.

7. Гуров С. В., Уткин Л. В., Надежность систем при неполной информации. СПб.: Любавич, 1999. 160 с.

УДК 621.39
ГРНТИ 49.37

РАНЖИРОВАНИЕ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ СИСТЕМЫ СВЯЗИ

О. М. Лепешкин, К. О. Мануков, М. А. Остроумов, О. А. Остроумов, С. В. Титов

Военная академия связи

Одним из свойств связи является безопасность, свойством системы связи устойчивость, при это при развертывании системы связи в любых условиях воздействия на нее дестабилизирующих факторов должно обеспечиваться ее устойчивое и безопасное функционирование. Принятый в 2017 году Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры (КИИ) Российской Федерации», вводит понятие критичности информационной инфраструктуры и ее объектов. Одним из этапов определения перечня объектов критической информационной инфраструктуры является процесс присвоения им категории важности. Для определения, какой из объектов субъекта критической информационной инраструктуры является наиболее важным можно провести процедуру ранжирования по важности. В работе представлены некоторые подходы к ранжированию объектов по важности.

критическая информационная инфраструктура, критически важный объект, безопасность информации, система управления.

В условиях развитие общества, новых технологий, цифровизации жизни люди, работники, так и руководители различных организаций, ведомств хотят получать и передавать информацию в любой момент времени. Процесс управления также подразумевает обмен информацией (данными) между управляющим и управляемым. В этом случае должна обеспечиваться

безопасность обмена, а также функциональная устойчивость системы в которой происходит обмен. Выход из строя отдельных элементов или (и) системы в целом может привести к срыву управления и к тяжелым последствиям вплоть до гибели людей. Устойчивость функционирования системы связи является критичной для системы управления и процесса управления. Сохранение функциональной устойчивости в условиях воздействие на систему различных дестабилизирующих факторов является очень важным, особенно для силовых ведомств, ядерной, энергетической, химической промышленности, а также в других сферах жизнедеятельности государства. Рассматривая вопрос критичности системы связи, которая состоит из различных взаимосвязанных элементов, необходимо четко понимать, что есть критичные объекты для системы, а есть не критичные, не влияющие на возможность ее функционирования, кроме этого критичные объекты тоже делятся по важности. Для определения важности необходимо проведение ранжирования критически важных объектов инфраструктуры (КВОИ).

Относительно недавно, в 2017 году принят ФЗ №187 «О безопасности критической информационной инфраструктуры Российской Федерации». В нем разъединяется, что включает критическая информационная инфраструктура (КИИ), какой объект является значимый. Основной угрозой для КИИ являются компьютерные атаки (КА). Изучением критической информационной инфраструктуры (КИИ), значимых объектов КИИ обеспечением их безопасности, устойчивости посвятили свои работы разные авторы [1, 2, 3, 4]. Еще одним более широким понятием, учитывающим важность объектов системы, является КВОИ, которое в большей степени встречается в локальных актах Министерства чрезвучайных ситуаций. В [5] рассматривается необходимость категорирования объектов КИИ по пяти показателям значимости и трем категориям, однако нет подходов к ранжированию по важности элементов объекта, объектов входящих в систему. При ранжировании объектов КИИ и КВО необходимо учитывать большое количество показателей.

В работе рассмотрим различные подходы к ранжированию объектов КВО и КИИ. Под ранжированием будем понимать расстановку элементов системы по рангу, признакам значимости, масштабности [6]. Основанием ранжирования будем понимать одно или несколько свойств объекта, по которым происходит упорядочение. Ранговый коэффициент значение, выраженное математически или аналитически, характеризующее основание ранжирования объекта.

Для ранжирования используют различные методы: оценки экспертов (методы ранжирования, приписывания баллов, формальные), расстановки приоритетов, согласования по критериям, с использованием формул Фишберна, анализа иерархий, интуитивно-рациональный (эвристический),

натурных экспериментов, моделирования и т. д. Чаще используют несколько методов, например, метод оценки экспертов и формулы Фишберна.

Эвристический метод основан использовании здравого смысла и интуиции лица, которое занимается ранжирования объектов. Данный метод основывается сугубо на компетенции должностного лица, его опыте. Имеет широкое применение, особенно в случае, если отсутствуют соответствующие средства для использования других методов.

Методы логико-вероятностного моделирования. Используются имитационные и аналитические модели. Как правило система представляет собой граф, состоящий из ее элементов и связи между ними. Способом моделирования воздействия на отдельные элементы (группу) определяется значимость их для работоспособности системы.

Широкое применение нашел метод экспертных оценок, который напоминает эвристический [7], однако, в отличие от него, используется специально созданная группа (один) специалистов, которой предоставляют перечень объектов, критерии и показатели оценки. Каждый эксперт размещает все объекты по рангу по шкале значимости. Полученные результаты заносят в таблицу, вычисляют сумму рангов, нормируют показатели

$$y_{ij} = \frac{\sum_{j=1}^{k} x_{ij}}{\sum_{j=1}^{k}\sum_{i=1}^{m} x_{ij}},$$

где x_i – значение i-го частного показателя,

k – количество экспертов,

m – количество частных показателей,

j – характеризует номер эксперта.

Аналогично производится ранжирование по методу приписывания баллов (метод непосредственного определения усреднения экспертных оценок) [7]. экспертам предлагается шкала для оценок, показатели и перечень объектов, которые необходимо оценить, при этом допускается присвоение показателям дробных значений, а также присвоение одинакового балла разным показателям. Вес каждого показателя рассчитывается по той же формуле, что и для метода ранжирования. При использовании каждым экспертом своей шкалы каждый показатель усредняется по строке, используя формулу

$$x_{ij} = \frac{c_{ij}}{\sum_{i=1}^{m} c_{ij}},$$

где c_{ij} – результат экспертной оценки i-го параметра j-м экспертом, а значение $\sum_{i=1}^{m} x_{ij}$ должно быть равно единице. Весовые коэффициенты каждого показателя, исходя из баллов экспертов, а также нормированные весовые коэффициенты рассчитываются как и в методе ранжирования. На достоверность полученных результатов влияет количество и качество вопросов, компетентность и количество экспертов и т. д.

Ранжирование объектов можно проводить путем попарного сравнения представленных экспертам объектов по представленной экспертам шкале [8]. Более важному в паре объекту присваивается целочисленное значение c, а менее важному $1/c$. После строится матрица парных сравнений и находится ранг объекта путем пошагового приближения к точным оценкам. Для этого на первом шаге значения веса каждого объекта принимается одинаковым (один делится на количество ранжируемых объектов). Вычисляют взвешенную сумму элементов строк матрицы, умножая каждый элемент строки на вес объекта. Нормируем по сумме (каждую взвешенную сумму, полученную в строках матрицы на первом шаге делим на сумму всех взвешенных сумм). Полученные значения – веса объектов на первом шаге. На втором шаге производится аналогичное вычисление весов. Примерно на 6–7 шаге значения практически не меняются. Полученные значения используются для определения ранга объекта.

Особенностью работы с группами экспертов является необходимость четкого ограничения задач исследования и постоянного контроля руководителя, определяющего вектор работы группы. Кроме этого необходимо учитывать уровень компетентности каждого эксперта.

Ранжирование с использованием графического метода, предполагает построение графа и его матрицы смежности [9]. Ранг определяется через степень доминирования по выражению $S = D + D^2$, где D – матрица доминирования. Для описания систем связи используются графы с петлями, а описывают их матрицы смежности. Ранг вычисляют из выражения $R = A + A^2$. Весовые коэффициенты (ранги) для каждого объекта будут равны R_i равны сумме в каждой стоке матрицы R.

При таком подходе к ранжированию возникает трудность в определении важности элементов с одинаковым рангом, а также не учитывает в полной мере одно- и двух звеньевые пути графов. В этом случае матрицу непосредственных путей преобразуют, добавляя по диагонали единицы и возводят в 2 и более степень, при этом чем выше степень, тем точнее результат, однако возведение в степень более 5 не рационально, т. к. значения рангов практически не меняются. Для вычисления рангов используют выражение:

$$R(i)=\left(\sum_{j=1}^{m}x_{ij}\right)/\sum_{i=1}^{m}\sum_{j=1}^{k}x_{ij},$$

где m характеризует положение элемента в строках матрицы, а k в столбцах.

Данный метод довольно просто реализуем и также может использоваться для определения важности элементов телекоммуникационных систем.

Еще одним часто используемым методом ранжирования являются формулы Фишберна [10, 11] применяются, если показатели уже упорядочены от наиболее важного к менее важному. В этом весовые коэффициенты i-го объекта представляют собой убывающую арифметическую прогрессию и определяются как

$$y_i=\frac{2(m-i+1)}{m(m+1)},$$

где m – количество показателей.

При строгом ранжировании показателей весовые коэффициенты подчиняются геометрической прогрессии, когда наиболее важным оказывается первый показатель для усиления простого линейного упорядочения

$$\begin{Bmatrix} y_1 \ge y_2+y_3+\ldots y_m \\ y_2 \ge y_3+y_4+\ldots y_m \\ \ldots \\ y_{m-1} \ge y_m \end{Bmatrix}$$

значения весов определяются как $y_i=\frac{2^{m-i}}{2^m-1}$, где $i=\overline{(1,m)}$.

Если известны интервалы возможных значений весовых коэффициентов для каждого i-го показателя x_i, то используется выражение

$$y_i=\alpha_i+\frac{1-\sum_{i=1}^{m}\alpha_i}{\sum_{i=1}^{m}(\beta_i-\alpha_i)}(\beta_i-\alpha_i),$$

где $\beta_i \;\; y_i \;\; \alpha_i$, $\beta_i>\alpha_i$, $\sum_{i=1}^{m}\alpha_i \;\; 1$, $\sum_{i=1}^{m}\beta_i \;\; 1$.

Особенностью использования данного метода является отсутствие необходимости обращения к экспертам, простота расчета, а также учет дополнительной информации (интервалы изменения весовых коэффициентов).

Актуальность вопроса деления (ранжирования) объектов по важности обусловлена деятельностью государства в области обеспечения безопасности инфраструктуры. Принятый в 2017 году ФЗ № 187 ввел понятийный аппарат КИИ РФ и определил требование по категорированию объектов КИИ, при этом не учитывается важность отдельных элементов, а категорирование проводится только по пяти категориям значимости. Для учета большего количества параметров объекта, определяющих его категорию важности необходимо использовать различные методы. Представленные в работе методы определения ранга позволяют ранжировать по важности объекты КИИ и КВО. При этом для обеспечения более точного ранжирования по важности объектов требуется использовать несколько методов.

Список используемых источников

1. Климов С. М., Поликарпов С. В., Рыжов Б. С., Тихонов Р. И., Шпырня И. В. Методика обеспечения устойчивости функционирования критической информационной инфраструктуры в условиях информационных воздействий // Вопросы кирбербезопасности. 2019. № 6. С. 37–48.

2. Янников И. М., Телегина М. В., Габричидзе Т. Г., Болтовский А. В. Реализация системы оценки безопасности КВ и потенциально опасных объектов // Известия Самарского научного центра Российской академии наук. 2018. Т. 20, № 6. С. 395–401.

3. Лепешкин О. М., Гаппоев Р. С. Оптимизация структуры комплекса технических средств в информационно-управляющих системах государственного управления // Научно-техничекие ведомости СПбГПУ. 2011. № 5. С. 129–132.

4. Груздев Д. А., Закалкин П. В., Кузнецов С. И., Тесля С. П. Мониторинг информационно-телекоммуникационных сетей // Труды учебных заведений связи. 2016. Т. 2. № 4. С. 46–50.

5. Федеральный закон от 26.07.2017 N 187-ФЗ “О безопасности критической информационной инфраструктуры Российской Федерации”.

6. Приказ Роспотребнадзора от 25.04.2012 № 193 “Об утверждении Методических рекомендаций по проведению инвентаризации объектов накопленного экологического ущерба”.

7. Методы определения весовых коэффициентов. URL: https://gigfbaza.ru/doc/31750.html (дата обращения 15.10.2020)

8. Воробьев С. Н., Балдин К. В. Системный анализ и управление рисками в предпринимательстве. М.: Издательство Московского психолого-социального института, 2009. 760 с.

9. Нечипоренко В. И. Структурный анализ и методы построения надежных систем. М.: Сов. радио, 1968. 255 с.

10. Баранов Ю. Г. Методы принятия управленческих решений. Псков: ПГУ, 2013. 176 с.

11. Хованов Н.В., Федотов Ю.В. Модели учета неопределенности при построении сводных показателей эффективности деятельности сложных производственных систем // Научные доклады. № 28. Изд-во Спб.: НИИ менеджмента СпбГУ, 2006. 37 с.

УДК 004.852
ГРНТИ 28.23.37

ОБ ИСПОЛЬЗОВАНИИ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РЕШЕНИЯ ЗАДАЧИ РАСПОЗНАВАНИЯ ОБРАЗОВ

В. Л. Литвинов, Е. А. Новиков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается задача распознавания образов как задача минимизации эмпирического риска при заданных условиях (в формулировке В. Н. Вапника). Исследуется возможность применения нейронных сетей для решения данной задачи. Показано несоответствие применяемых на практике функций потерь необходимым условиям. Также рассматриваются некоторые возможные варианты функций потерь, соответствующие условиям задачи. Для таких функций приводится эксперимент, доказывающий предположение о слабой применимости нейронных сетей прямого распространения для решения задачи распознавания образов.

распознавание образов, регрессия, статистическая теория обучения, минимизация эмпирического риска, машинное обучение, нейронные сети, многослойный персептрон, градиентные методы минимизации, градиентный спуск.

Задача распознавания образов, хотя и является одной из первых задач машинного обучения (одна из первых её постановок была предложена в [1]), но до сих пор является крайне актуальной. Отчасти актуальность данной задачи обосновывается тем, что с теоретической точки зрения она является простейшей задачей обучения [2].

Прежде чем приступать к исследованию, необходимо отметить следующее. Несомненно, распознавание образов на данный момент является обширной областью машинного обучения [3] и включает в себя крайне большое количество различных методов, алгоритмов (например, Байесовские классификаторы, и многое другое). Однако данная работа имеет опосредованное отношение к теории распознавания образов. Нас будет интересовать только постановка задачи распознавания образов, данная В. Н. Вапником в работе [2], к которой мы и будем постоянно обращаться. В частности, мы будем исследовать, соответствует ли этой постановке задачи тот метод, на основе которого задачу распознавания образов решают нейронные сети.

Основываясь на информации из различных пособий по нейронным сетям [4, 5] можно считать, что на практике чаще всего применяются градиентные методы обучения. Все последующие рассуждения будут относиться именно к обучению нейронных сетей прямого распространения с помощью методов, основанных на использовании градиента.

Итак, рассмотрим математическую постановку задачи распознавания образов [2, 6].

В некоторой среде, которая характеризуется распределением вероятности $P(x)$, случайно и независимо происходят события x ($x \in \mathbb{R}^n$). Эти события некоторый «учитель» относит к одному из k классов (без ограничения общности можно считать, что $k = 2$), исходя из некоторого правила, которое можно понимать как распределение вероятности $P(\omega \mid x)$, где $\omega = \{0, 1\}$ ($\omega = 0$, если событие принадлежит первому классу; $\omega = 1$, если второму). Ни $P(x)$, ни $P(\omega \mid x)$ априорно не известны, однако они гарантированно существуют. Для упрощения записи, без ограничения общности, можно считать, что задана вероятность $P(x, \omega)$.

Кроме того, задано также множество решающих правил $\varphi(x, \alpha)$, $\alpha \in \Lambda$. В таком случае, рассмотрим функцию потерь $L(\omega, \varphi(x, \alpha)) = Q(z, \alpha)$, где $z \in \mathbb{R}^{n+1}$ – вектор, состоящий из всех значений x и значения ω, причем $Q(z, \alpha)$ принимает только 2 значения: 0 и 1.

Тогда задача распознавания образов состоит в минимизации функционала

$$R(\alpha) = \int Q(z, \alpha) dP(\omega, x)$$

при условии, что распределение $P(\omega, x)$ неизвестно, но дана выборка пар

$$(\omega_1, x_1), ..., (\omega_l, x_l).$$

Именно условие того, что функция потерь $Q(z, \alpha)$ может принимать всего 2 значения, позволяет считать задачу распознавания образов простейшей задачей статистического обучения.

Однако в практическом использовании (даже для решения задачи распознавания образов, например [7]) нейронные сети, вообще говоря, работают с функциями потерь, которые выдают вещественные значения. При решении задач распознавания образов с помощью нейронных сетей обучение проводят именно на вещественных значениях, а при использовании обученной сети получаемые значения либо округляют, либо используют как вероятность принадлежности образа классу.

Пример выполнения программы, которая так решает задачу распознавания образов можно видеть на рис. 1. Значение «cross valid round» – это значение ошибки классификации на валидационном наборе данных при

округлении функции активации выходного слоя (0 – первый класс, 1 – второй класс). На рис. 2 можно видеть процесс сходимости обучения (это стоит отметить, это будет необходимо в дальнейшем).

Однако, хотя этот метод и используется обычно на практике, строго говоря, он не подпадает под условия задачи распознавания образов. Действительно, поскольку функция ошибки может принимать не только значения 0 или 1, то это решение некоторой иной задачи. В той же работе [2] описывается и такая задача – задача восстановления регрессии – для нее $Q(z, \alpha)$ имеет значения в $\mathbb{R}$ и $A \leq Q(z, \alpha) \leq B$. При этом задача регрессии включает в себя задачу распознавания образов.

```
python program.py

Число внутренних слоев: 1
Число нейронов в каждом слое: 10
Функция активации: sigm
loss value: 0.05435825139284134
cross valid: 0.051006391644477844
cross valid round: 0.04999999701976776
```

Рис. 1. Пример решения задачи распознавания образов с помощью поиска регрессии

Основываясь на вышеизложенном, можно сделать вывод, что нейронные сети на практике решают, строго говоря, не задачу распознавания образов, а задачу восстановления регрессии.

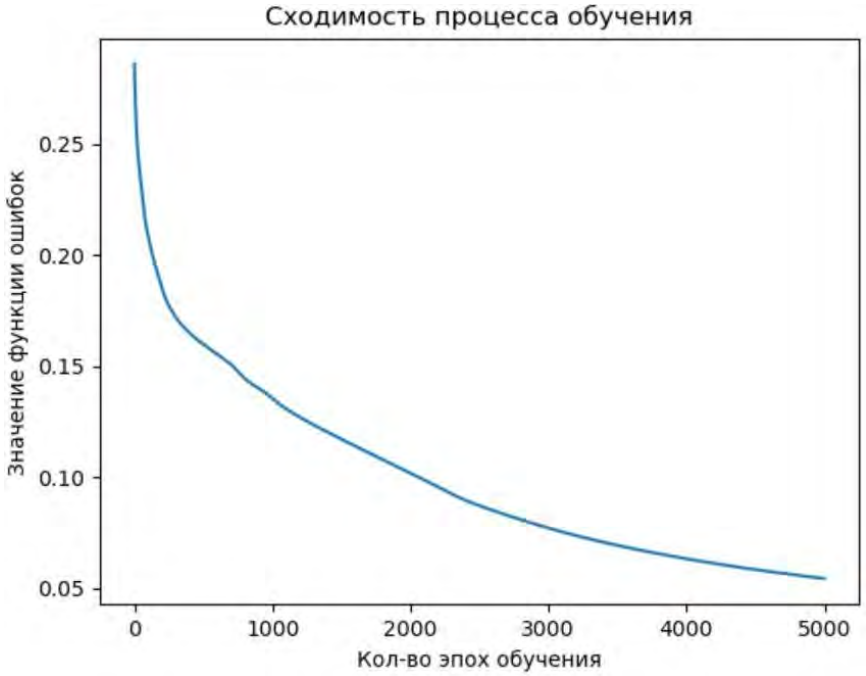


Рис. 2. Сходимость обучения нейронной сети при решении задачи регрессии

Но если нейронные сети способны решать задачу регрессии (которая является более общей), то, возможно, они способны решать задачу распознавания образов и непосредственно, а не как подзадачу? Действительно, если в процессе обучения передавать в функцию ошибки округленное значение, то она будет иметь в качестве возможных значений только 0 и 1, что вполне будет соответствовать требованиям задачи распознавания образов.

Проведен эксперимент, исследовавший возможность решения задачи распознавания образов с помощью нейронных сетей. Для этого использовалась та же нейронная сеть, результаты обучения которой показаны на рис. 1 и 2, лишь с тем изменением, что после применения функции активации полученное значение округлялось. Результаты обучения можно видеть на рис. 3 и 4.

Как можно видеть из этих рисунков, при попытке решения задачи распознавания образов алгоритм обучения не сходится к минимальному значению.

```
python program.py

Число внутренних слоев: 1
Число нейронов в каждом слое: 10
Функция активации: sigm
loss value: 0.699999988079071
cross valid: 0.699999988079071
```

Рис. 3. Решение задачи распознавания образов с помощью нейронной сети

Можно сделать предположение, что это связано с тем фактом, что при поиске оптимальных значений весов для нейронной сети на каждом шаге вычисляется значение градиента в текущей точке и делается шаг в противоположном ему направлении. А поскольку при использовании округленных функций процесс обучения должен сходиться аналогично рис. 5, то можно сделать вывод, что градиент в каждой точке равняется либо нулю, либо бесконечно велик. В таком случае, вероятность сходимости процесса обучения к какому-то значению будет равновероятна угадыванию всех весов нейронной сети, которые позволяют достигать это значение (поскольку градиент всегда будет нулевой, и движение по поверхности ошибки не будет происходить).

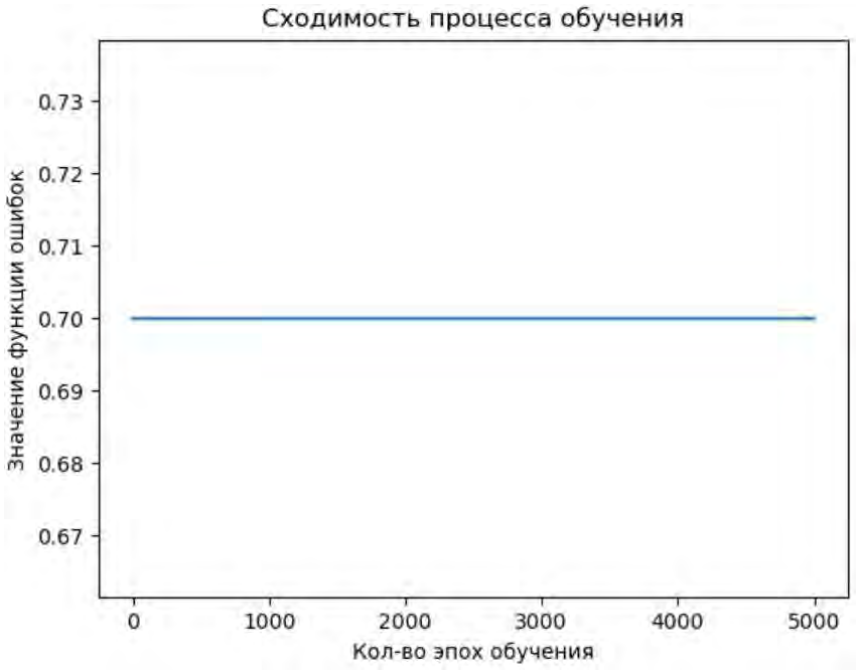


Рис. 4. Сходимость обучения нейронной сети в задаче распознавания образов

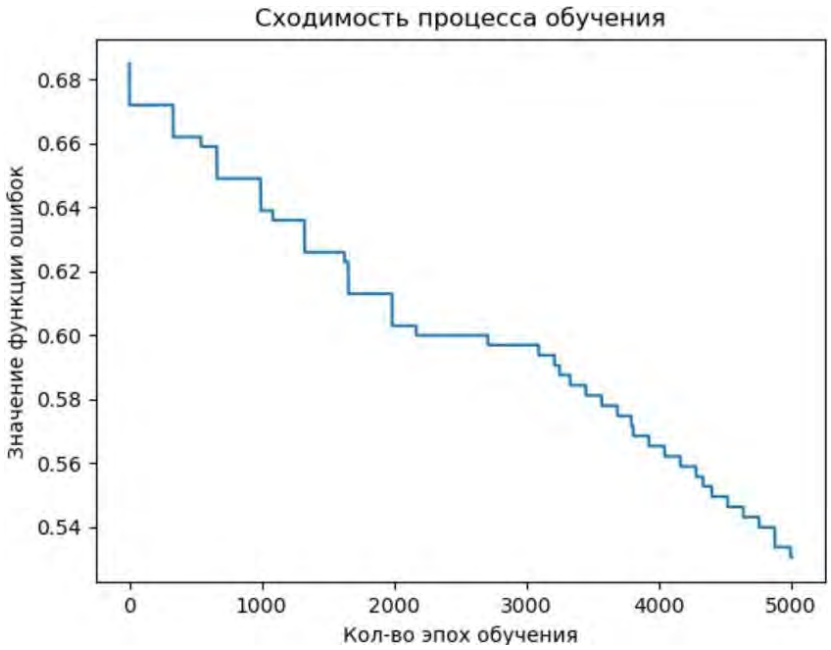


Рис. 5. Предположительная сходимость обучения нейронной сети в задаче распознавания образов (методом без применения градиента)

Основываясь на результатах проведенного эксперимента и высказанном предположении можно заключить, что нейронные сети прямого распространения, использующие градиентные методы обучения не приспособлены решать задачу распознавания образов непосредственно, а способны только как подзадачу задачи восстановления регрессии.

Список используемых источников

1. Браверман Э. М. Опыты по обучению машины распознаванию зрительных образов // Автоматика и телемеханика. 1962. № 3. С. 349–364.

2. Vapnik V. N. Statistical Learning Theory. N.Y.: J. Wiley, 1998. 736 с.

3. Фукунага К. Введение в статистическую теорию распознавания образов: пер. с англ. М. : Наука, 1979. 368 с.

4. Хайкин С. Нейронные сети: полный курс: пер. с англ. 2-е изд. М. : Издательский дом «Вильямс», 2006. 1104 с.

5. Гудфеллоу Я., Бенджио И., Курвилль А. Глубокое обучение: пер. с англ. М. : ДМК Пресс, 2018. 652 с.

6. Вапник В. Н., Червоненкис А. Я. Теория распознавания образов (статистические проблемы обучения). М. : Наука, 1974. 416 с.

2. Макхман Б., Рао Д. Знакомство с PyTorch: глубокое обучение при обработке естественного языка : пер. с англ. СПб.: Питер, 2020. 256 с.

УДК 004.852
ГРНТИ 28.23.37

ПРОРЕЖИВАНИЕ НЕЙРОННЫХ СЕТЕЙ ПРЯМОГО РАСПРОСТРАНЕНИЯ С ПОМОЩЬЮ АЛГОРИТМОВ OBS И L-OBS

В. Л. Литвинов, Е. А. Новиков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается способ обучения нейронных сетей прямого распространения путем их прореживания, то есть удаления нейронных связей. Исследуются алгоритмы Optimal Brain Surgeon (OBS) и Layer-wise Optimal Brain Surgeon (L-OBS). Изучается влияние процедуры прореживания на обученную нейронную сеть, в частности изучается значение функции ошибки после применения этой процедуры. Показан положительный результат применения рассматриваемых алгоритмов, а также превосходство алгоритма L-OBS над алгоритмом OBS. В дополнение рассматривается влияние процедуры прореживания нейронной сети на оценочную VC-размерность данной сети.

машинное обучение, нейронные сети, многослойный персептрон, прореживание нейронных сетей, OBS, Optimal Brain Surgeon, VC-размерность.

Прореживание нейронной сети – метод уменьшения числа используемых в нейронной сети весов путем удаления наименее релевантных. В результате прореживания сети число параметров может значительно уменьшаться (из-за чего увеличивается скорость работы и уменьшается необходимый объем памяти) при одновременном уточнении результата. Об актуальности данной темы и широте дискурса можно судить по статье [1].

Вообще говоря, существуют различные методы прореживания нейронных сетей. Основное различие методов прореживания заключается в выборе критериев определения удаляемых весов нейронной сети. В данной работе будут рассматриваться методы, основанные на использовании информации о второй производной функции ошибки – гессиана.

Изначально идея использовать гессиан была описана в работе [2], однако алгоритм Optimal Brain Damage (OBD), предлагавшийся в этой работе, был слабо применим, поскольку предполагал гессиан диагональным для увеличения скорости его расчета. В работе [3] был предложен алгоритм Optimal Brain Surgeon (OBS), позволявший работать с недиагональным гессианом без ухудшения времени работы, что привело к значительному улучшению результатов работы нейронных сетей по сравнению с OBD.

В дальнейшем были предложены различные модификации алгоритма OBS (например [4, 5]), однако в данной работе они рассматриваться не будут. С точки зрения структуры нейронной сети наиболее интересным представляется алгоритм Layer-wise Optimal Brain Surgeon (L-OBS), представленный в работе [6]. Именно он будет рассматриваться в данной работе вместе с исходным алгоритмом OBS.

Итак, рассмотрим непосредственно алгоритм OBS.

Разложим функцию ошибки в ряд Тейлора по переменной весов нейронной сети до третьей степени. Получим следующее приближение:

$$dE = \left(\frac{\partial E}{\partial \mathbf{w}}\right)^T \cdot d\mathbf{w} + \frac{1}{2} d\mathbf{w}^T \cdot \mathbf{H} \cdot d\mathbf{w} + O(\|d\mathbf{w}\|^3),$$

где $\mathbf{H} = \partial^2 E/\partial \mathbf{w}^2$ – гессиан. После обучения нейронной сети обычными градиентными методами (например, с помощью градиентного спуска) имеем $(\partial E/\partial \mathbf{w})^{\mathrm{T}} \cdot d\mathbf{w} \approx 0$. Таким образом, необходимо используя информацию из $\mathbf{H}$ и $d\mathbf{w}$ найти такой элемент w_q вектора $\mathbf{w}$, чтобы при замене $w_q = 0$ значение dE возрастало минимально.

Не вдаваясь в детали (которые в полной мере описаны в работе [3]), можно получить, что элементу w_q вектора $\mathbf{w}$ соответствует параметр «выпуклости» L_q, который определяет влияние этого элемента на значение dE, причем

$$L_q = \frac{1}{2} \frac{w_q^2}{\left[\mathbf{H}^{-1}\right]_{qq}},$$

где $[\mathbf{H}^{-1}]_{qq}$ – элемент с индексами q,q матрицы, обратной гессиану $\mathbf{H}$. Таким образом, рассчитав значения L_q для каждого веса нейронной сети можно определить наименее значимые (с наименьшим значением L_q) и удалить их (либо определенное число весов, либо не превышающие какое-либо значение, либо определенных иным способом).

Алгоритм L-OBS дополняет исходный алгоритм следующим образом.

Прежде всего, в работе [6] показывается, что функция E ошибки всей сети линейно зависит от функций ошибки каждого отдельного слоя (из-за громоздкости формула не приводится). Кроме того, показывается, что содержательная часть гессиана (использующаяся для алгоритма) может высчитываться без расчета всего гессиана, а из этой части можно получить содержательную часть матрицы, обратной гессиану (необходимой для расчета L_q). Таким образом, алгоритм L-OBS позволяет получать более «гибкие» данные (поскольку веса каждого слоя оптимизируются раздельно), причем с уменьшением времени расчета, сравнительно с алгоритмом OBS.

Далее, перейдем к экспериментальной части. Будем рассматривать задачу классификации (число классов $k = 2$), а решать ее будем с помощью нейронных сетей прямого распространения (как простейших нейронных сетей). Рассматривать будем относительно простые нейронные сети [7]: с тремя внутренними слоями (число нейронов каждого внутреннего слоя выберем не очень большим, около 15), в качестве функции активации будем использовать сигмоидальную функцию (как одну из простейших). Для простоты эксперимента создадим специальные (относительно простые) наборы – графические представления этих наборов можно видеть на рис. 1 (каждое число – некоторый элемент рассматриваемого множества, причем этот элемент принадлежит к классу с номером этого числа). Сходимость обучения на этих наборах следует из их линейной разделимости.

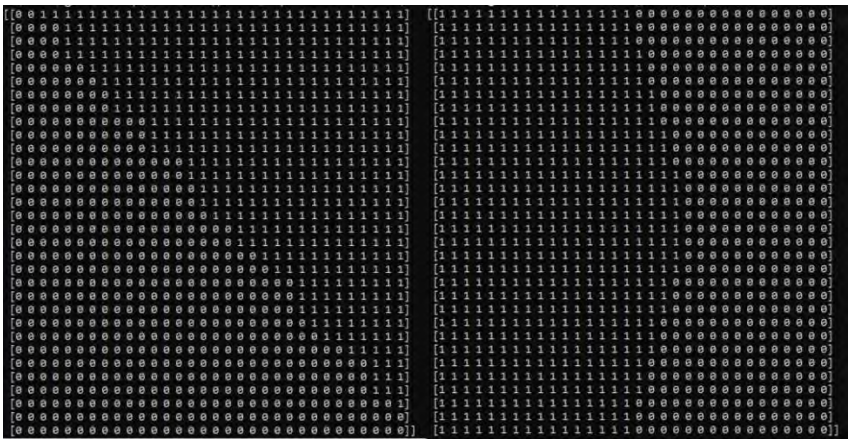


Рис. 1. Наборы данных, использующиеся в экспериментах

Все дальнейшие эксперименты проводились на обоих приведенных наборах данных. Для любого утверждения относительно результатов эксперимента подразумевается, что оно имеет место на обоих наборах (с относительно малыми изменениями), если не указано обратного.

Далее, изучим, является ли актуальным алгоритм L-OBS (прежде чем переходить к его экспериментальному исследованию). Т. е., рассмотрим, имеет ли место значительное различие (в один или несколько порядков) между значениями параметра выпуклости для весов различных слоев сети.

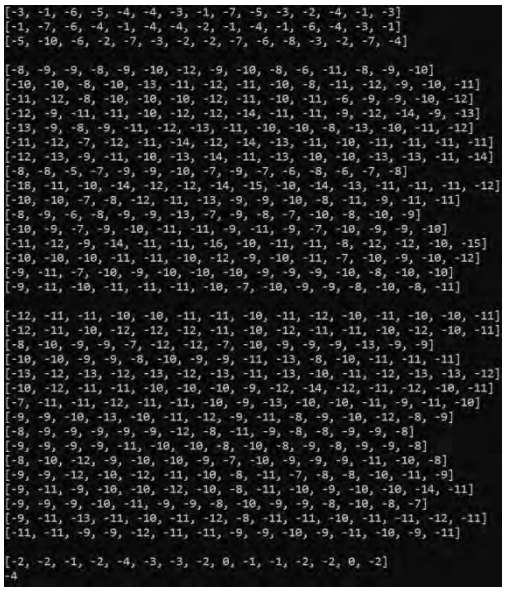


Рис. 2. Порядки значений параметров выпуклости Lq для 3хслойной нейронной сети

Для этого обучим нейронную сеть с тремя внутренними слоями. Обучим её и рассчитаем параметр выпуклости L_q для её весов. На рис. 2 приведен результат этого расчета, причем выведены порядок значения при основании 10 (пустыми строками разделены слои, последняя строка для каждого слоя определяет значения смещения b_{li}). Как можно видеть, значения для второго и третьего слоя обычно колеблются в диапазоне от 10^{-15} до 10^{-7}, при диапазоне 10^{-7} – 10^{-2} для первого и последнего. Это вполне оправдывает необходимость применения алгоритма L-OBS.

На рис. 3 и 4 можно видеть экспериментальные результаты работы алгоритмов OBS и L-OBS соответственно (кроме значений функции потерь на обучающей и валидационной выборке также выводится число единиц – незатронутых весов – и размер применяемой для прореживания маски).

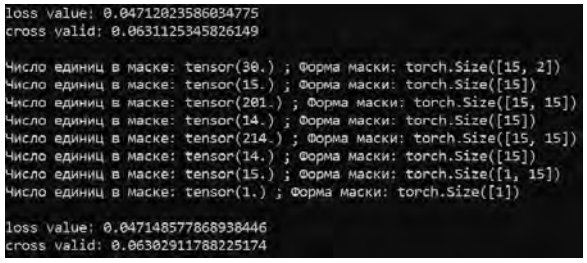


Рис. 3. Результаты работы алгоритма OBS

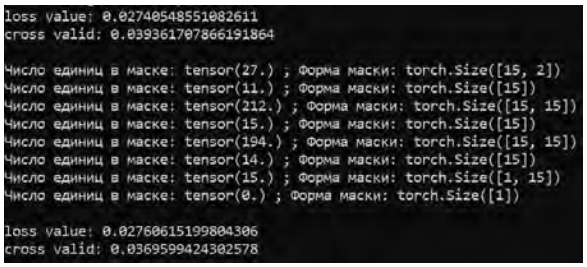


Рис. 4. Результаты работы алгоритма L-OBS

При выборе удаляемых значений использовались следующие пороговые значения: для алгоритма OBS – значение функции потерь (*loss value*) * $2*10^{-11}$; для алгоритма L-OBS – *loss value* * $2*10^{-4}$ для слоя 1, *loss value* * $2*10^{-11}$ для слоя 2, *loss value* *10^{-11} для слоя 3, *loss value* * $2*10^{-3}$ для выходного слоя.

Как можно видеть, после прореживания в обоих случаях увеличилось значение функции потерь, но уменьшилось значение функции потерь на валидационном наборе (*cross valid*). При этом значение *cross valid* для алгоритма L-OBS уменьшилось на несколько тысячных, а для алгоритма OBS на несколько стотысячных (т. е. различие в 2 порядка), что позволяет заключить о превосходстве алгоритма L-OBS. При этом алгоритм L-OBS удалил большее число весов, что позволяет сделать нейронную сеть менее громоздкой при улучшении результатов ее работы. Чтобы определить, насколько итоговые сети отличаются друг от друга по сложности структуры, воспользуемся формулой из работы [8], согласно которой для нейронной сети F ее VC-размерность высчитывается как

$$VCdim(F) \le 2W \log_2(eN),$$

где W – число весов в нейронной сети,

N – число узлов (количество применений функций активации),

e – основание натурального логарифма.

Получаем, что для изначальной сети F_0 размерность ограничивалась как $VCdim(F_0) \leq 7537.5$, а после применения алгоритма OBS имеем $VCdim(F) \leq 7022$, а после применения L-OBS $VCdim(F) \leq 6799.1$. То есть OBS уменьшил число на 515.5, а L-OBS – на 738.1, иначе говоря, алгоритм L-OBS работает лучше алгоритма OBS на (738.1-515.5)/515.5 = 0.43 или на 43 %.

Таким образом, алгоритм L-OBS позволяет получать приближение итоговых значений на порядки лучше алгоритма OBS при 43% улучшении оптимизации структуры сети.

Список используемых источников

1. Blalock, D.; Ortiz, J.; Frankle, J.; Guttag, J. What is the State of Neural Network Pruning? // 2020. URL: https://arxiv.org/abs/2003.03033 (дата обращения 06.02.2021)

2. Le Cun, Y.; Denker, J.; Solla, S. Optimal Brain Damage // Advances in Neural Information Processing Systems. 1989. N 2. Pp. 598–605.

3. Hassibi B., Stork D. Second order derivatives for network pruning: Optimal Brain Surgeon // International Joint Conference on Neural Networks. 1992. N 5. Pp. 164–171.

4. Attik, M.; Bougrain, L.; Alexandre, F. Optimal Brain Surgeon for Feature Selection // Advances in Neural Information Processing Systems. 2004. N 2.

5. Larsen J., Hansen L., Svarer C., Ohlsson M. Design and Regularization of Neural Networks: the Optimal Use of a Validation Set // Neural Networks for Signal Processing. 1996

6. Xin D., Shanhyu C., Sinno P. Learning to Prune Neural Networks via Layer-wise Optimal Brain Surgeon // 2017. URL: https://arxiv.org/abs/1705.07565 (дата обращения 06.02.2021)

7. Хайкин С. Нейронные сети: полный курс: пер. с англ. 2-е изд. М. : Издательский дом «Вильямс», 2006. 1104 с.

8. Baum E., Haussler D. What Size Net Gives Valid Generalization? // Advances in Neural Information Processing Systems. 1988. N 1. Pp. 81–90.

УДК 004.932
ГРНТИ 28.23.15

ИССЛЕДОВАНИЕ МЕТОДОВ РАСПОЗНАВАНИЯ АГРЕССИВНОГО ПОВЕДЕНИЯ НА ВИДЕОИЗОБРАЖЕНИЯХ

В. Л. Литвинов, И. Ю. Раднаева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В то время как проблема распознавания действий стала часто обсуждаемой темой в компьютерном зрении, идентификация агрессивного поведения в целом изучена сравнительно меньше. Автоматизированное распознавание на видеоизображениях такого вида поведения человека даст полезный эффект в некоторых сценариях видеонаблюдения, в частности, в тюрьмах, школах, психиатрических центрах или иных подобного рода учреждениях. В статье проведено исследование некоторых методов компьютерного зрения, позволяющих идентифицировать дисфункции поведения человека для целей своевременного оповещения о чрезвычайной ситуации и предотвращения негативных последствий агрессивного поведения.

агрессивное поведение, компьютерное зрение, распознавание образов, сверточные нейронные сети.

Агрессивное поведение – это одна из форм реагирования на различные неблагоприятные в физическом и психическом отношении жизненные ситуации, вызывающие стресс, фрустрацию и подобные состояния [1].

Основной функцией масштабных систем видеонаблюдения, развернутых в таких учреждениях, как тюрьмы, школы, психиатрические центры и ряде иных, является предупреждение ответственного персонала о потенциально опасной ситуации и предотвращение плачевных исходов. Тем не менее, операторы изрядно перегружены количеством изображений с камеры, а время отклика вручную слишком велико. Сложившаяся ситуация приводит к высокому спросу на автоматические системы оповещения, а также системы тегов, которые могут обрабатывать огромное количество видеоинформации, загруженной на веб-сайты [2].

В общем смысле при распознавании объектов на видеоизображениях происходит процесс детектирования движений человека на кадрах видеоряда, процесс двигательной активности представляется в видеопотоке как пространственное изменение значений пикселей, которые относятся к визуальным объектам на каждом кадре (рис. 1).

Рис. 1. Процесс распознавания двигательной активности человека

На вход системы выделения признаков поступают кадры видеопотока, после чего в блоке выделения признаков выполняется отбор наиболее значимых пространственно-временных признаков визуальных объектов на обрабатываемых кадрах согласно выбранным дескрипторам [3]. Выбранные признаки поступают на вход блока анализа динамики признаков, а в дальнейшем происходит их классификация, в частности отнесение двигательной активности к агрессивному поведению человека.

Группа тайваньских ученых [4] осуществила распознавание выстрелов, взрывов и торможение автомобилей как визуально, так и в аудио, с использованием иерархического подхода, основанного на сочетании метода Гаусса и скрытых марковских моделей (СММ).

Алгоритм обучения в СММ только максимизирует отклик каждого изображения на свою модель, но не минимизирует отклик на иные модели. Например, после инициализации СММ начинается работа с изображением, оно просматривается сверху вниз, и модель последовательно переходит из одного состояния в другое (рис. 2). Далее для каждого изображения из базы строится своя СММ, а задача нейронной сети будет заключаться в сравнении исходного изображения с шаблонным посредством вычисления вероятности с помощью алгоритма прямого-обратного хода [5].

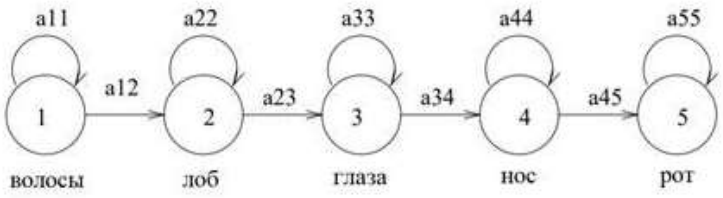


Рис. 2. Разделение области лица на значимые части

С большей вероятностью лидерами в достижении наиболее эффективных результатов в области распознавания изображений следует признать сверточные нейронные сети (СНС), состоящие из конволютивных слоев, каждый их которых применяет фильтр к картинке для выявления структурных особенностей. Первые несколько слоев обнаруживают более крупные

особенности, например, диагональные линии, а последующие слои коллекционируют более тонкие детали, организованные в более сложные функции.

Локальные элементы изображения, или точки интереса, обеспечивают компактное и абстрактное представление модели изображения. Аналогичным способом можно определить компактное представление движения. Однако использование только СНС может привести к значительной потере времени для произведения вычислений. В этом случае целесообразно применять подход переноса знаний, при котором глубокая искусственная нейронная сеть сначала обучается на выборке большого размера, а затем используется в качестве экстрактора признаков. После этого полученные признаки используются для обучения классификатора [3]. Архитектура такой нейросети представлена на рис. 3.

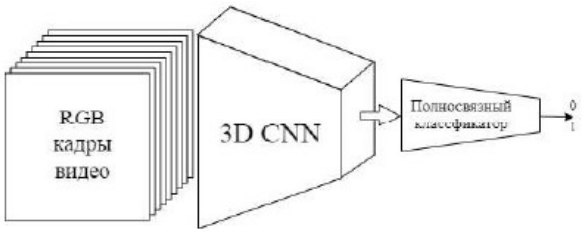


Рис. 3. Обобщенная архитектура нейросетевой системы на основе 3D CNN

Основной визуальной подсказкой для обнаружения агрессии будет являться функция расчета псевдо-кинетической энергии для *j*-го человека, обеспечивающая единую меру интенсивности артикуляционных движения человека:

$$\bar{E}_j = \frac{1}{Q}\sum_{q=1}^{Q}\left|v_q\right|^2,$$

где v_q – инвариантный вектор скорости для $q = 1\ldots Q$.

Если в кадр попадает несколько объектов, предполагается, что человек с наивысшим значением $\bar{E}_j$ идентифицируется в окружающей обстановке как проявляющий агрессию. Тогда выходная характеристика псевдо-кинетической энергии окружающей среды φ_k на временном отрезке k рассчитывается следующим образом:

$$\varphi_k = \max_j \bar{E}_j = \bar{E}_{jmax}.$$

Кроме того, взаимодействие наблюдаемого объекта с другими людьми на видеоизображении также является индикативным для выявлении агрессивного поведения. Резкое движение конечностью считается более агрессивным, если объекты стоят, однако то же движение в сидячем положении

может рассматриваться, как безобидное размахивание руками во время беседы. Измерение взаимодействия ξ_k на временном шаге k затем вычисляется как минимальное евклидово расстояние между отслеживаемым положением наиболее энергичного человека j_{max} и набором L_{jmax}, содержащим местоположения всех других отслеживаемых объектов:

$$\varepsilon_k = \min_{l \in L_{jmax}} [D^E(l, t^1_{j_{max}})].$$

Таким образом, набор L содержит заранее определенное местоположение объектов, представляющих интерес на изображении, в результате чего действия даже со стороны одного человека могут быть определены как агрессивное поведение.

Далее обозначим индекс дискретного времени $k = 1, 2, \ldots$, и установим приращение времени 50 мс. На k-ом шаге $\psi^c_k \in \{0,1\}$ свойства аудио идентификатора класса $c \in \{\text{речь, крики, пение, звуки удара}\}$. φ_k определяет характеристики псевдо-кинетической энергии окружающей среды, ε_k измеряет взаимодействие между объектами. Если принять за a_k уровень агрессии на шаге k и описать стохастический процесс $\{a_k\}$ с динамикой, заданной марковской сетью первого порядка, тогда вероятность перехода между состояниями будет задана функцией:

$$p(a_{k+1} = i | a_k = j) = \text{CPT}^a(i, j).$$

Вычисленные визуальные (φ_k, ε_k) и аудиальные ($\psi_k = \{\psi_{ck}\}$) характеристики рассматриваются как образцы из распределения наблюдений, которое зависит от уровня агрессии a_k. Однако наблюдения не могут происходить в идеальных условиях, поэтому следует ввести скрытую переменную индикатора шума $n_k \in \{0,1\}$. Тогда модель будет представлена в виде функций условной вероятности для признаков визуальной агрессии CPT^{φ} и CPT^{ε}, а также функций условной вероятности $\text{CPT}^{\psi c}$ для обнаружения аудио класса ψ^c:

$$p(\varphi_k = i | a_k = j) = \text{CPT}^{\varphi}(i, j)$$
$$p(\varepsilon_k = i | a_k = j) = \text{CPT}^{\varepsilon}(i, j)$$
$$p\,\psi^c_k = i | a_k = j, n_k = n) = \text{CPT}^{\psi^c}(i, j, n).$$

На основе описанной методики из датасета, содержащего 25 видеорядов, 13 из которых действительно содержали сцены агрессивного поведения объекта, получены результаты (табл.).

ТАБЛИЦА. Сравнение методов

№ п/п	Метод определения агрессивного поведения	Содержит сцену агрессии	Истинно положительный	Ложно положительный
1	Аудио характеристики	13	7	2
2	Характеристики кинетической энергии	13	4	5
3	Комбинация 1+2	13	6	4
4	Комбинация 2+Видео характеристики	13	10	5
5	Комбинация 4+1	13	11	5

Результат сравнительного анализа методов определения агрессивного поведения представлен в диаграмме (рис. 4).

В заключении хотелось бы отметить, что в целях идентификации случаев агрессивного поведения и последующего предотвращения его последствий следует использовать современные технологии компьютерного зрения и соответствующие методы идентификации объектов на видеоизображениях. Исходя из проведенного анализа, наиболее высокую эффективность несут комбинированные методы: сочетание аудио, видео и характеристик кинетической энергии.

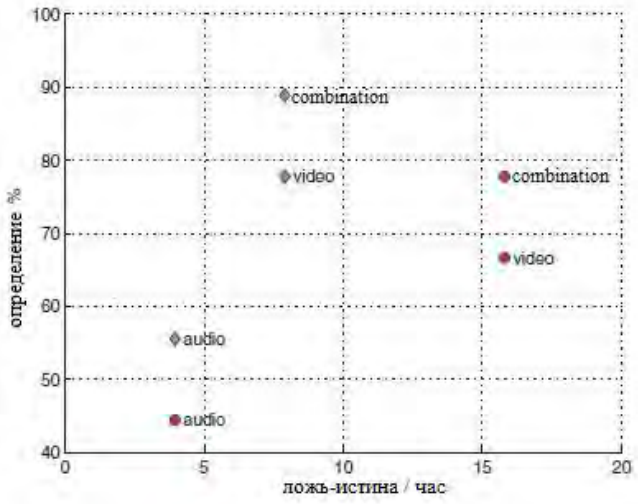


Рис. 4. Сравнительный анализ методов определения агрессивного поведения

Список используемых источников

1. Мещеряков Б., Зинченко В. Агрессия // Большой психологический словарь / сост. Олма-пресс, 2004.

2. Bermejo, E.; Deniz, O.; Bueno, G.; Sukthankar, R. Violence Detection in Video Using Computer Vision Techniques // CAIP 2011: Computer Analysis of Images and Patterns. pp. 332–339.

3. Уздяев М. Ю. Распознавание агрессивных действий с использованием нейросетевых архитектур 3D-CNN // Известия ТулГУ. Технические науки. 2020. Вып. 2.

4. Cheng, W. H.; Chu, W. T.; Wu, J. L.: Semantic context detection based on hierarchical audio models. In: Proceedings of the ACM SIGMM workshop on Multimedia information retrieval. 2003. Pp. 109–115.

5. Хлопенкова А. Ю., Рыбкин С. В. Исследование алгоритмов распознавания образов на основе геометрических точек и скрытых марковских моделей // Международный

студенческий научный вестник. 2018. № 6. URL: http://www.eduherald.ru/ru/ article/view?id=19245 (дата обращения 25.01.2021).

УДК 004.855.5
ГРНТИ 28.23.37

АВТОМАТИЗАЦИЯ МЕТОДОВ ЛИТОЛОГО-ФАЦИАЛЬНОГО АНАЛИЗА ПОСРЕДСТВОМ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ

В. Л. Литвинов, Д. И. Руйго

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Исследование направлено на анализ методов литолого-фациального анализа нефтегазоносных толщ на предмет их автоматизации посредством применения современных технологий машинного обучения. В данной работе изучены существующие достижения специалистов геологических и информационных наук в области применения интеллектуальных методов обработки геологических данных на различных этапах литолого-фациального анализа нефтегазоносных толщ, определены актуальные проблемные ситуации и задачи по внедрению средств машинного обучения.

литолого-фациальный анализ, геологоразведка, машинное обучение, классификация, нейронные сети.

Современные задачи поиска нефтяных месторождений требуют применения все более сложных и объемных методов сбора и анализа данных геологоразведки. Один из методов сбора данных по месторождениям – литолого-фациальный анализ – сталкивается с задачами составления фациальных карт на участках со сложными геологическими обстановками шельфовых зон. Дороговизна сбора разведывательных данных для составления моделей месторождений с высокой детализацией и большие объемы обрабатываемых данных ставят перед научным сообществом задачи по поиску новых методов анализа геологических данных, базирующихся на применении современных интеллектуальных технологий.

Целью работы является поиск проблемных ситуаций и задач по внедрению средств машинного обучения с целью автоматизации этапов литолого-фациального анализа нефтегазоносных толщ.

На первом этапе исследования изучена структура литолого-фациального анализа, определены его этапы, цели и задачи каждого из этапов. Всего выделяют 5 этапов литого-фациального анализа [1]:

1) Выбор стратиграфического горизонта;
2) Всестороннее изучение литологических и палеонтологических характеристик отложений;
3) Выделение фаций внутри изучаемого горизонта;
4) Составление карт фаций горизонта;
5) Составление палеогеографической карты.

Каждый этап анализа оперирует различными данными. На втором этапе исследования определены этапы, данные которых поддаются машинной обработке (II-V этапы). Для каждого этапа определены виды и типы данных, представленные в таблице.

ТАБЛИЦА. Соответствие типов данных этапам литолого-фациального анализа

Этап анализа	Вид данных	Тип данных
II этап	Данные каротажа	Спектрограмма
	Сейсмические данные	Спектрограмма
	Данные керна	Изображения (видимые диапазон, УФ-диапазон)
III этап	Классифицированные данные II этапа	Числовой и логический
IV этап	Кластеризованные данные III этапа	Числовой, вектор
V этап	Картографические данные IV этапа	Числовой, вектор

Идентификация и классификация типов данных позволяет провести подбор методов машинной обработки данных, которые потенциально могут повысить автоматизацию этапов литолого-фациального анализа. Для наглядности развития исследования составлена его концептуальная модель, представленная на рис.

На третьем этапе проведен анализ существующих исследований, направленный на выявление проблемных ситуаций и актуальных задач автоматизации этапов литолого-фациального анализа.

Работа специалистов университета Альберты, направленная на автоматизацию кластеризации каротажных данных методом *K*-средних в сочетании с отсеиванием аномальных значений, показала, что разработанный метод позволяет относительно быстро получить представление по изучаемым данным, однако в отдельных случаях получаемое количество кластеров субъективно [2].

Исследование, проведенное в Исследовательском геофизическом обществе (Потсдам) в 2020 году, показало что классификация фаций (сейсмический разрез) методом опорных векторов (SVM) достигает точности 0,983 ± 0,004 [3]. Достигнутый результат указывает на высокую точность

синтезированной модели, сопоставимую с результатами достигаемых традиционными методами.

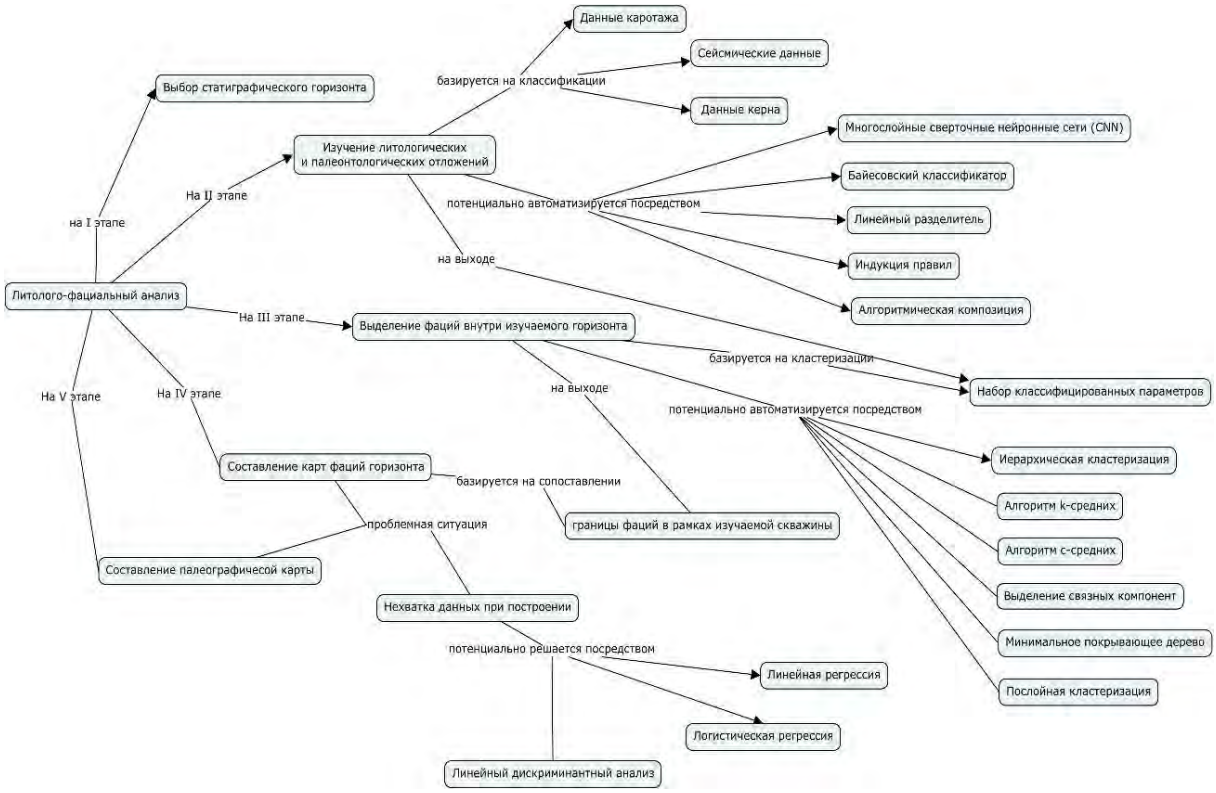


Рис. Концептуальная модель исследования

Специалисты Сколковского университета в 2019 году разработали несколько моделей классификаторов горных пород, основанные на сверточных нейронных сетях ResNet и GoogleNet. Достигнута точность 70–72 % [4]. Анализ ложно-положительных и ложно-отрицательных классификаций выявил возникновение ошибок при классификации литотипов со схожей структурой.

Помимо применения моделей, базирующихся на сверточных нейронных сетях, в ряде работ проведено исследование классификаторов более низкого порядка сложности. Так в 2016 году в Научно-Техническом Центре «Газпромнефти» был разработан классификатор литолого-фациальных обстановок, базирующийся на спектральной теории. Выявлено, что использование для классификации *EM*-алгоритма дает возможность не только строить карты классов, но и охарактеризовать надежность полученной классификации. Разработанная в исследовании методика позволила упростить задачу геолога при выделении фаций, значительно снизила время на построение фациальных карт и сократила влияние субъективного фактора [5].

Высокие показатели точности показывает применение рекурентных нейронных сетей в задаче интерпретации геофизических исследований

скважин. Предварительный экспертный анализ пропущенных интервалов показал, что разработанная модель позволяет выделить на 14 % больше дополнительных эффективных толщин, чем анализ, представленный экспертами [6].

Таким образом, анализ существующих научных исследований показал, что интеллектуальные методы обработки информации (методы машинного обучения) обеспечивают достаточно высокое качество интерпретации и обработки данных. Наиболее широко на данный момент изучены методы классификации и кластеризации фаций (на основе данных каротажа, сейсморазведки и изучения керна). Анализ материала позволил выявить проблемные ситуации, решение которых на данный момент не определено в достаточной мере.

В качестве проблемных ситуаций можно выделить задачу классификации литотипов со схожей структурой, а также наукоемкую задачу повышения уровня точности классификации горных пород посредством применения современных моделей сверточных нейронных сетей и задачу автоматизации построения карт фаций горизонта посредством применения моделей, основанных на рекурентных нейронных сетях.

Список используемых источников

1. Алексеев В. П. Литолого-фациальный анализ: Учебно-методическое пособие к практическим занятиям и самостоятельной работе по дисциплине "Литология". Екатеринбург: Изд-во УГГГА, 2003.147 с.

2. Ibinabo Bestmann, Facies classification using unsupervised machine learning in geoscience // DATA SCIENCE IN OIL AND GAS, 2020. URL: https://towardsdatascience.com/facies-classification-using-unsupervised-machine-learning-in-geoscience-8b33f882a4bf (дата обращения 24.01.2021).

3. Thilo Wrona, Seismic facies analysis using machine learning // GEOPHYSICS Volume 83, Issue 5, 2018. URL: https://library.seg.org/doi/full/10.1190/geo2017-0595.1 (дата обращения 27.01.2021).

4. Barboshkin Evgeny E. Deep convolutions for in-depth automated rock typing // Computers & Geosciences. Volume 135, 2019. URL: https://www.researchgate.net/publication/335989937_Deep_Convolutions_for_In-Depth_Automated_Rock_Typing (дата обращения 27.01.2021).

5. Хасанов М. М. Автоматизация литолого-фациального анализа на основе спектральной теории // Нефтяное хозяйство. Апрель 2016. С. 48–51.

6. Егоров Д. В., Буханов Н. В. Экспертный анализ геолого-физической информации по Приобскому и Муравленковскому месторождениям на основе моделей машинного обучения // Нефтяное хозяйство. Январь 2018. С. 28–31.

УДК 004.492.3:004.056.57
ГРНТИ 81.93.29

АЛГОРИТМ РАСПОЗНАВАНИЯ ПОЛИМОРФНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ARM-СИСТЕМ НА ОСНОВЕ ДИНАМИЧЕСКОГО АНАЛИЗА

Д. О. Маркин, В. М. Миначёв

Академия Федеральной службы охраны Российской Федерации

В статье приводится алгоритм анализа трасс выполнения программ для процессоров ARM архитектуры. Построена модель вредоносного программного обеспечения. Разработана схема отнесения программы к вредоносной и метод обнаружения подозрительного поведения Проведена оценка эффективности метода по разработанному прототипу программного средства.

динамический анализ, эксплойт, шелл-код, ассемблерный код, полиморфный код.

Популярность современных вычислительных систем на базе процессоров с архитектурой *ARM* постоянно растет. Соответственно, растет и количество программного обеспечения (ПО) для данных систем, в том числе, вредоносного. Данные обстоятельства требуют своевременного совершенствования моделей вредоносного программного обеспечения (ВПО), а также алгоритмов его распознавания, учитывающих особенности *ARM*-систем [1]. Архитектура *ARM* имеет ряд специфических особенностей по сравнению с привычной *Intel x86/64.* Ряд известных методов анализа, разработанные для процессоров других архитектур, не применимы к *ARM* [2]. Поэтому требуются новые подходы и средства анализа ПО на основе особенностей *ARM* архитектуры.

Вопросами безопасности ПО в данной области занимается большое число отечественных и иностранных исследователей. Построением средств анализа и выявления ВПО для ARM-систем уделено внимание в работах Гайворонской С. А. [2], Гамаюнова Д. Ю. и Сковороды А. А. [3, 4]. Последние использовали динамический анализ для распознавания ВПО. Вопросами оценки соответствия ПО для мобильных устройств уделено внимание в работах Маркова А. С., Горюнова М. Н. и Мацкевича А. Г. [5, 6]. Среди иностранных экспертов известны труды Jagsir S. [7], Costan V. [8], Pinto S. [9**Список используемых источников**

] и др.

Современные методы чаще всего применяют техники, построенные для технологий прошлых поколений, основанные на статическом анализе с применением машинного обучения. Основные минусы этих методов – ложные корреляции и слабая способность обнаружения полиморфного кода. Применение динамического анализа и шаблонов поведения позволит повысить эффективность существующих систем анализа ПО.

Выделение поведенческих признаков и начальное тестирование программного средства осуществлялось на основе следующих наборов данных:

– набор полезных нагрузок эксплойтов базы данных *www.exploit-db.com*;

– *ELF*-файлы каталога */bin Unix*-подобной системы *Raspbian GNU/Linux 10* аппаратной платформы *ARMv6*;

– содержимое секции *.text* (код выполняемой программы) файлов предыдущего пункта.

Требуется разработать алгоритм способный распознать вредоносное ПО полиморфной структуры по шаблонам поведения и иным косвенным признакам.

Программы использующие уязвимости различного рода с целью нарушения основных свойств информации, называются эксплойтами. После успешной реализации уязвимости запускается полезная нагрузка эксплойта, наиболее распространенной является шелл-код. Обычно он позволяет получить доступ к программной оболочке системы с правами доступа, в случае *Linux* это *bash*. Любой системный вызов начинается с команды *svc* с заранее определенным параметром, перед этим запуском регистры *r0-r14* должны иметь определённые значения, принудительно присваиваемые им командой *mov*. Для защиты от статического исследования и скрытия процесса вызова системного прерывания, описанного выше, применяется полиморфизм. Полиморфный код заключается в алгоритме расшифрования (зашифрования) кода полезной нагрузки, обычно он представляет собой функции получения и использования значения регистра *pc* (текущего адреса инструкции), загрузки (*ldr*), применения арифметических инструкций (*xor, eor, sub*) и выгрузки (*str*) обратно в память шелл-кода. При запуске шелл-кода с помощью переполнения буфера не допускается наличие нулевых байтов, которые при копировании строки интерпретируются как конец строки. Для решения этой проблемы злоумышленники применяют переход с 4-х байтного размера команд (*arm mode*), на 2-х байтный (*thumb mode*), в следствии чего повышается число бесполезных инструкций для выравнивания кода по 4 байта, или просто обнуляющих инструкций без применения переменной #0, например – *subs r2, r2, r2*.

Разработанный алгоритм обнаружения обрабатывает адрес, вызываемые инструкции и значения регистров, совокупность этих параметров назы-

вается трассой выполнения программы *T*. В результате анализа *T* полученные показатели передаются на схему принятия решения *S*, которая относит программу к вредоносной, или к безопасной. В *T* выделяются поведенческие признаки полиморфного кода и статического шелл-кода. Для этого *T* рассматривается как последовательность трансформированных шаблонов *W*, которая состоит из элементов множества элементов $\{P_1, \ldots, P_8\}$. Все инструкции трассы *T* относятся к одной из восьми категорий, представленных шаблонами P_i этого множества, соответственно:

1. Если инструкция записывает в один или несколько регистров значение из диапазона значений адресного пространства эмулируемого кода, она относится к шаблону P_1 (функция получения *pc* кода);

2. Если инструкция использует пару регистр-значение, которая получена от предыдущей инструкции, удовлетворяющей шаблону P_1, она относится к шаблону P_2 (функция использования *pc* кода);

3. Если инструкция производит чтение из памяти по адресу из диапазона значений адресного пространства эмулируемого кода, то она относится к шаблону P_3 (*ldr*);

4. Если инструкция производит запись в память по адресу, используемому последней инструкцией, удовлетворяющей шаблону P_3, она относится к шаблону P_4. Переход по этой ветви обозначает успешный разбор автоматом A_1 последовательности *W* (*str*);

5. Инструкции, не относящиеся к предыдущим шаблонам, относятся к шаблону P_5 (обработка данных и др.);

6. Если инструкция помещает в регистр значение не из адресного пространства эмулируемого кода, то она относится к шаблону P_6;

7. Если выполняемая инструкция – *svc*, то она относится к шаблону P_7. Переход по этой ветви обозначает успешный разбор автоматом A_2 последовательности *W*;

8. Инструкции, не относящиеся к шаблонам P_1, P_2, P_6, P_7 относятся к шаблону P_8.

На основе отнесения инструкции к той или иной категории строятся автоматы A_1 и A_2. Если последовательность *W* разбирается автоматом A_1, подтверждается наличие полиморфного кода, а наличие шелл-кода – автоматом A_2. Обнаружение последовательности расшифровщик-шелл-код осуществляется передачей адреса последней инструкции, успешно разобранной атоматом A_1, на вход автомату A_2 как адрес первой анализируемой инструкции начального состояния. Успешный разбор *W* автоматами A_1 и A_2 представленны на рис. 1.

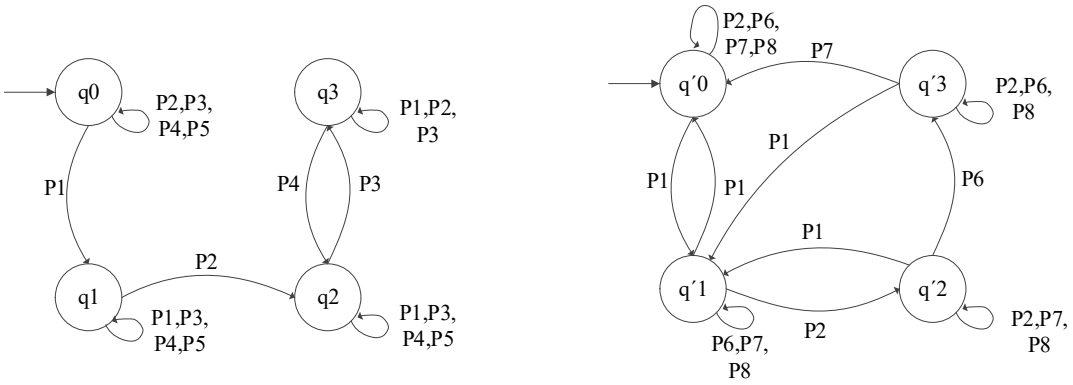


Рис. 1. Пример успешного разбора W автоматами A_1 и A_2

В прототипе программного средства применяется *CPU* эмулятор *Unicorn* [10], это позволит избежать вредоносного воздействия эксплоита и большой нагрузки на аппаратную составляющую, так как объем виртуальной оперативной памяти будет контролируем. Фреймворк дизассемблирования *Capstone* [11] позволит сформировать трассу в привычном виде. Модульная схема разработанного средства представлена на рис. 2.

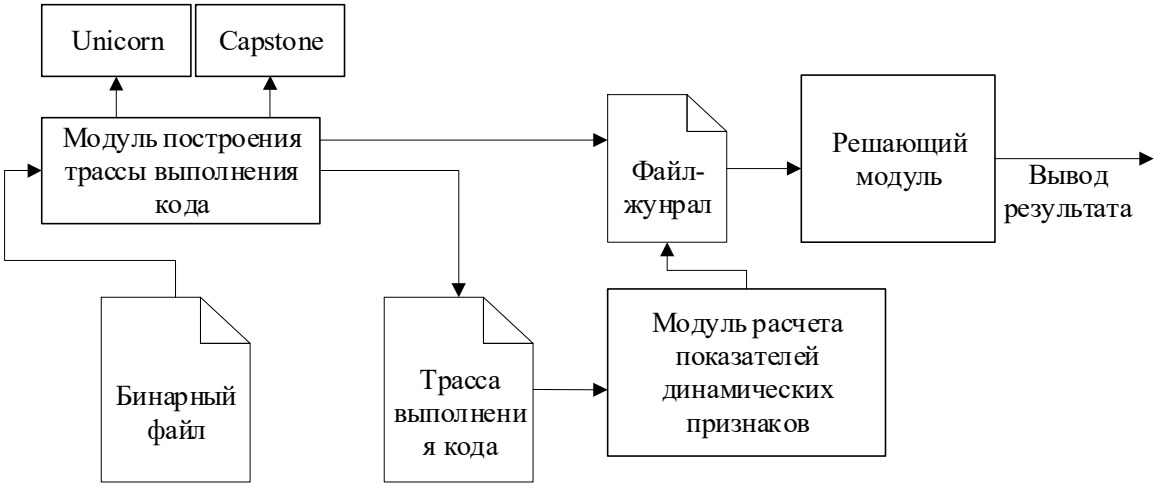


Рис. 2. Схема программного средства анализа

Модуль построения трассы выполнения кода (модуль 1) загружает файл в виртуальную оперативную память. После каждого этапа выполнения инструкции происходит сравнение текущей инструкции с инструкцией в бинарном файле. Количество таких несовпадений, объем файла и объем проанализированных данных записывается в файл журнал. Дизассемблированный код вместе с значениями регистров записывается в файл-трассу.

Модуль расчета показателей динамических признаков (модуль 2) производит подсчет числа бесполезных инструкций, не вносящих изменения в регистры общего назначения), количество инструкций получения и использования значения *pc* регистра, количество успешных разборов автоматами A_1 и A_2 последовательности W и общее число запущенных инструкций.

Решающий модуль (модуль 3) реализует схему принятия решения, структура данной схемы гибкая и возможно дальнейшее исследование и её изменение.

Эффективность алгоритма оценена на тестовой выборке данных, результаты представлены в таблице.

ТАБЛИЦА. Значение показателей эффективности алгоритма

Результат анализа / Анализируемые данные	Решение		Среднее покрытие кода
	Вредоносное ПО	Безопасное ПО	
Шелл-коды	81,4 %	18,6 %	47 %
Бинарные файлы	100 %	0 %	0,12 %
Исполняемый код бинарного файла	59,3 %	40,7 %	0,02 %

Предварительная подготовка данных снизила покрытие кода и вероятность ошибки первого рода (59,3 %). Причина высокой вероятности ошибки первого рода состоит в низком покрытии кода. Низкое покрытие кода вызвано неспособность эмулятора обрабатывать полезную нагрузку, что приводи к остановке эмуляции. Увеличение покрытия кода осуществляется повторным запуском процесса эмуляции с адреса последнего прерывания. Замена эмулятора на виртуальную машину не допустимо, так как полезная нагрузка шелл-кода может вывести из строя машину, что приведет к непредусмотренной перезагрузке. Часть ошибок второго рода также возникла из-за системного прерывания выполняемого кода, объясняемое невозможностью эмулятора процессора выполнить полезную нагрузку. Из-за этого средство анализа не смогло собрать достаточную информацию о трассе выполнения бинарного файла.

Список используемых источников

1. Маркин Д. О., Миначев В. М. Анализ особенностей исполнения приложений в доверенной среде исполнения на основе технологии ARM TrustZone // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020): IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. Санкт-Петербург: СПбГУТ, 2020. Т. 2. 748 с. С. 515–520.

2. Гайворонская С. А., Гамаюнов Д. Ю. Гибридный метод обнаружения шеллкодов // Системы высокой доступности. 2012. Том 2, № 8. С. 33–44.

3. Гамаюнов Д. Ю., Сковорода А. А. Анализ мобильных приложений с использованием моделей привилегий и API-вызовов вредоносных приложений // Прикладная дискретная математика. 2017. № 36. С. 84-105. doi http://doi.org/10.17223/20710410/36/7.

4. Гамаюнов Д. Ю., Сковорода А. А. Динамический анализ мобильных приложений // Программная инженерия. 2019. № 7-8. С. 324–333. doi http://doi.org/10.17587/prin.10.324-333.

5. Горюнов М. Н. и др. Распознавание функциональных объектов программного обеспечения в условиях отсутствия исходных текстов // Информационные системы и технологии. 2013. № 5. С. 112–120.

6. Марков А. С., Цирлов В. Л., Барабанов А. В. Методы оценки несоответствия средств защиты информации / под ред. доц. А. С. Маркова. Москва : Радио и связь, 2012. 192 с.

7. Jagsir Singh Jaswinder Singh Detection of malicious software by analyzing the behavioral artifacts using machine learning algorithms // Information and Software Technology Volume 121, May 2020, p. 35.

8. Costan, V.; Lebedev, I.; Devadas, S. Sanctum: Minimal hardware extensions for strong software isolation // Proceedings of the USENIX Security Symposium. USENIX Association, 2016. Pp. 857–874.

9. Pinto, S.; Santos, N. Demystifying Arm TrustZone: A Comprehensive Survey // ACM Computing Surveys, 2019. January 10. p. 36.

10. Unicorn. The Ultimate CPU emulator. URL: https://www.unicorn-engine.org (дата обращения: 07.03.2021).

11. Capstone. The Ultimate Disassembler. URL: https://www.capstone-engine.org/lang_python.html (дата обращения 07.03.2021).

УДК 004.056.52
ГРНТИ 81.93.29

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ HASP ДЛЯ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОТ НЕАВТОРИЗОВАННОГО ИСПОЛЬЗОВАНИЯ

Д. О. Маркин, Е. А. Никифорова

Академия Федеральной службы охраны Российской Федерации

В работе описана технология защиты от несанкционированного использования информационной системы, доступ к ресурсам которой осуществляется удаленно, на основе использования технологии HASP, аппаратных идентификаторов – токенов, и технологии перехвата системных вызовов средствами параметра LD_PRELOAD.

информационная система, HASP, перехват системных вызовов, защита авторских прав.

Введение

В условиях решения задач по развитию цифровой экономики важным направлением является обеспечения безопасности информационных систем (ИС) и ресурсов, доступ к которым в может предоставляться удаленно.

Если способы и технологии ограничения доступа и защиты от несанкционированного доступа (НСД) и использования локально установленного программного обеспечения (ПО) исследованы достаточно хорошо, то защита авторских прав программного обеспечения информационных систем обладает определенной спецификой [1]. ПО ИС, как правило, разработано на интерпретируемых языках программирования, а значит – находятся в форме исходных текстов. Данное обстоятельство делает неприменимыми многочисленные классические методы защиты от известных средств и методов анализа [2]. С другой стороны, информационные ресурсы, как правило, хранятся в составе ИС в открытом виде. Данные обстоятельства позволяют при наличии возможности копирования данных защищаемой ИС, предоставлять доступ к ней нелегально, поскольку информационные технологии, лежащие в основе функционирования такой ИС, не содержат средств защиты от несанкционированного копирования и использования.

Одной из наиболее эффективных технологий защиты от несанкционированного использования в настоящее время является технология *HASP* (*Hardware Against Software Piracy*) [3]. Данная технология предполагает использования специальным образом настроенных аппаратных идентификаторов – токенов или *HASP*-ключей. Основные сервисы безопасности, реализуемые в *HASP*-ключах – идентификация и аутентификация, шифрование, разграничение доступа.

Основой технических средств *HASP*-ключей является специализированная индивидуальная (уникальная) микросхема – *ASIN* (*Application Specific Integrated Circuit*), обеспечивающая уникальный порядок вычислений для каждого ключа.

С точки зрения применения *HASP*-ключей в целях защиты ПО известно два способа: *Envelope* и *HASP API*.

Первый способ – *HASP Envelope* – позволяет реализовывать контроль наличия *HASP*-ключа, исключая НСД, выполнение политики безопасности и лицензирования, затруднение анализа машинного кода исходного алгоритма, применение обфускации и механизмов от отладчиков. *HASP Envelope* дает возможность распространять данные, которые защищенное приложение использует в процессе работы. Алгоритм защиты уникален для каждого разработчика и, соответственно, взломав одну защищенную программу, для следующей необходимо реализовывать взлом иначе.

Второй способ – *HASP API* – заключается в определении необходимых для защиты функций и их подключении из заранее подготовленных библиотек. В набор функций входят такие как кодирование, декодирование информации, контроль лицензии, контрольное суммирование, чтение и запись из памяти ключа, мониторинг работы и в сети и т. д. Данные способ менее

надежен так как при наличии известных способов обхода функционала, заложенного в применяемые библиотечные функции, отключение защиты осуществляется сравнительно оперативно.

Модель угроз

Задачами подсистемы защиты ИС являются:

1. Обеспечения блокирования доступа к информационным ресурсам ИС в случае копирования данных ИС неавторизованным пользователем, развертыванию в иной компьютерной системе и попытке предоставления доступа к ней некоторому кругу пользователей.

2. Обеспечения защиты от несанкционированного доступа к информационным ресурсам защищаемой ИС в случае копирования данных ИС неавторизованным пользователем.

Модель нарушителя

Предлагаемая схема использования технологии *HASP* для защиты ИС от неавторизованного использования направлена на защиту от квалифицированных пользователей, выполняющих функции системного администрирования ИС, т. е. от внутренних нарушителей.

Предполагается, что авторизованность доступа к информационным ресурсам защищаемой ИС обеспечивается наличием аутентичного *HASP*-ключа, подключенного к интерфейсам ЭВМ, на которой развернута защищаемая ИС.

Описание применения технологии HASP для защиты информационной системы от неавторизованного использования

Типовая схема применения технологии *HASP* показана на рис. 1.

В случае применения данной технологии для защиты ПО информационной системы от несанкционированного доступа и использования предлагается схема, представленная на рис. 2.

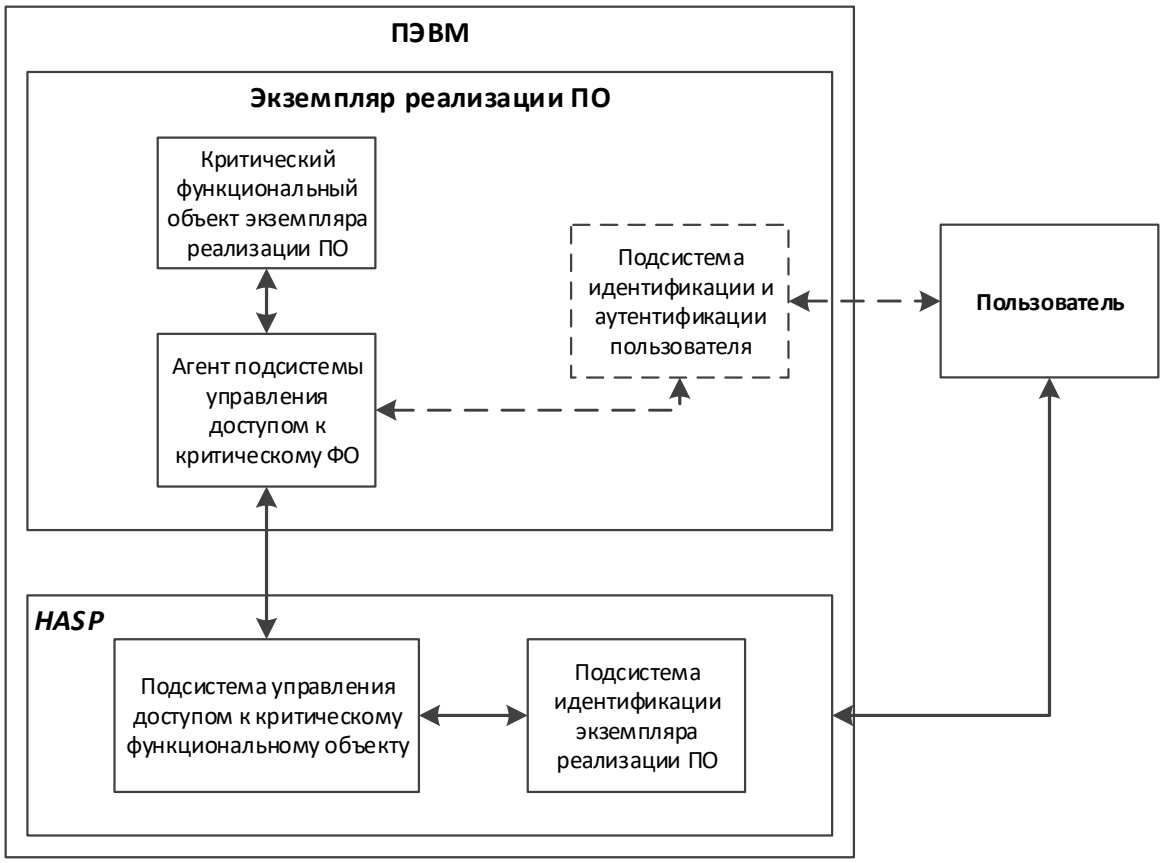


Рис. 1. Классическая схема защиты экземпляра реализации ПО
от несанкционированного использования средствами *HASP*-ключа

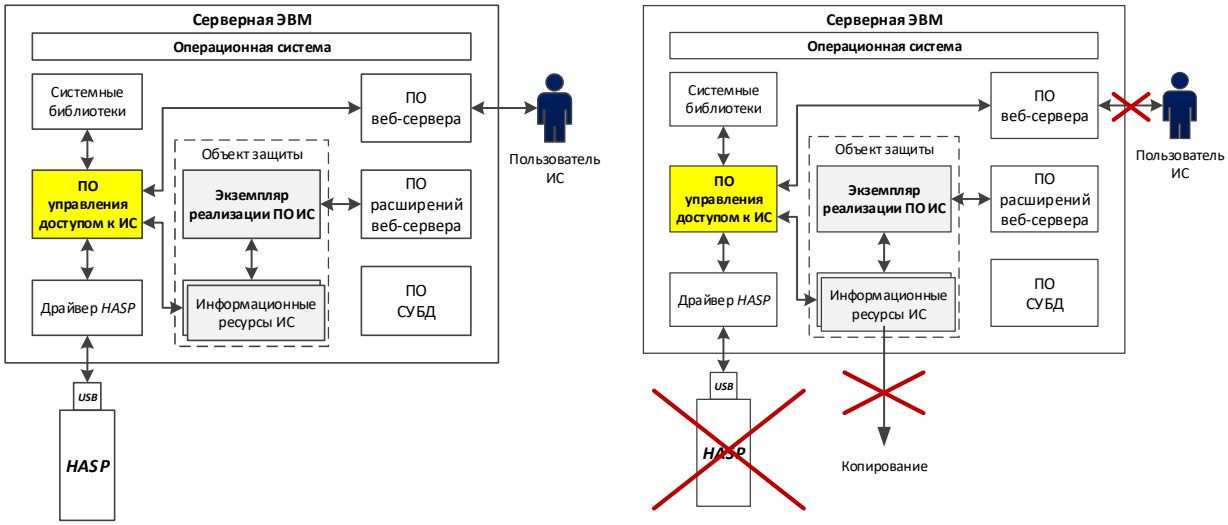


Рис. 2. Схема управления доступом
к информационным ресурсам средствами *HASP*-ключа:
а) при наличии *HASP*-ключа; б) в условиях отсутствия *HASP*-ключа

Особенности функционирования системы защиты предложенной схемы заключаются в следующем:

3. *HASP*-ключ выполняет функции аппаратного идентификатора для обеспечения авторизованного использования ПО ИС и средством криптографической защиты информационных ресурсов защищаемой информационной системы для обеспечения защиты данных ресурсов от несанкционированного копирования.

4. Наличие и аутентичность *HASP*-ключа проверяет дополнительный модуль управления доступом к ИС, который реализует функции проверки уникального идентификатора *HASP*-ключа (например, *ID* токена).

5. Модуль управления доступом к ИС обеспечивают реализацию следующих механизмов безопасности:

5.1. Защиту от несанкционированного доступа пользователей к информационным ресурсам ИС в случае отсутствия аутентичного *HASP*-ключа.

5.2. Защиту от копирования информационных ресурсов в случае отсутствия аутентичного *HASP*-ключа.

5.3. Обеспечение авторизованного доступа к информационным ресурсам ИС при наличии аутентичного *HASP*-ключа.

6. Обеспечение функции проверки наличия аутентичного *HASP*-ключа модуль управления доступом реализует средствами *API*-доступа в соответствии со стандартом *PKCS* 11 или *APDU*-протокола.

7. Обеспечение функции контроля доступа к информационным ресурсам ИС модуль управления доступом реализует в несколько этапов:

7.1. Устанавливает «ловушку» на системные вызовы операционной системы (ОС), реализующие стек протоколов *TCP*/*IP*.

7.2. Идентифицирует вызов обработчиков системных вызовов, предназначенных для обработки данных защищаемой ИС.

7.3. При наличии аутентичного *HASP*-ключа:

7.3.1. Обеспечивает расшифрование информационных ресурсов защищаемой ИС.

7.3.2. Предоставляет доступ к информационным ресурсам защищаемой ИС в соответствии с настроенной политикой разграничения доступом.

7.4. В случае отсутствия аутентичного *HASP*-ключа:

7.4.1. Блокирует доступ к информационным ресурсам защищаемой ИС либо искажает передаваемые данные.

7.4.2. Сигнализирует авторизованному пользователю защищаемой ИС о попытке несанкционированного использования.

В основе перехвата системных вызовов для разных операционных систем могут использоваться такие функции как *SetWindowsHook* – для ОС семейства *Windows* либо специальный параметр вызова программ *LD_PRELOAD* – для ОС семейства *UNIX*.

Выводы

Таким образом, основой системы защиты ИС от несанкционированного использования, а также информационных ресурсов ИС от несанкционированного доступа и копирования является модуль управления доступом, реализующим функции:

– прокси-сервера уровня прикладного программного обеспечения для обработки системных вызовов и функций из стека протокола TCP/IP;

– средства контроля наличия аутентичного HASP-ключа, подключенного к интерфейсу серверной ЭВМ;

– средства криптографической защиты информационных ресурсов ИС.

Список используемых источников

1. Жданова И. В., Быков Д. В. Варианты построения системы защиты электронных документов от копирования // Инженерный вестник Дона. 2012. № 8 (68). С. 490–492.

2. Маркин Д. О., Звягинцев С. А., Павлов Д. И. Методы и средства анализа программного обеспечения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019): VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2019. Т. 2. 603 с. С. 293–298.

3. Ананченко И. В., Мусаев А. А. Защита приложений, выполняемых торговым терминалом Metatrader, ключами Sentinel HASP // Труды СПИИРАН. 2013. № 3 (26). С. 69–78.

УДК 004.056.5
ГРНТИ 50.37.23

СПОСОБ ИДЕНТИФИКАЦИИ ТОЧЕК ВХОДА ОБФУСЦИРОВАННЫХ ВЕБ-ПРИЛОЖЕНИЙ СРЕДСТВАМИ МОДЕЛИРОВАНИЯ СЦЕНАРИЕВ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ

Д. О. Маркин, Д. А. Рыков

Академия Федеральной службы охраны Российской Федерации

В работе описан способ идентификации точек входа удаленных веб-приложений, формируемых обфускированным программным обеспечением, разработанным, как правило, на языке JavaScript и исполняющимся средствами веб-браузера. Предложенный способ позволяет повысить количество обнаруживаемых точек входа удаленных веб-приложений и более эффективно подготовить информационную модель сайта для ее

дальнейшего использования в рамках решения задач анализа защищенности и поиска уязвимостей методом фаззинга.

JavaScript, обфускация, деобфускация, эмуляторы кода, веб-приложения, фаззинг.

Решение задачи развития цифровой экономики требует совершенствования и создания новых информационных систем (ИС), выполняющих важные с точки зрения обеспечения интересов личности, общества и государства функции. Такие ИС, как правило, относятся к объектам критической информационной инфраструктуры [1], и поэтому вопросы обеспечения информационной безопасности (ИБ) данных систем, являются первоочередными, так как затрагивают принципиально важные. Анализ защищенности и выявление уязвимостей информационных системах может выполняться разными способами [2]. Один из наиболее эффективный – фаззинг – как метод автоматического поиска дефектов и ошибок программного обеспечения (ПО) [3]. Однако для эффективного фаззинга требуется наличие информации о внутренней структуре программного обеспечения, которая часто отсутствует.

К таким способам реализации фаззинга относятся:

– фаззинг с псевдослучайной генерацией входных данных;

– фаззинг с обратной связью, в т. ч. с применением интеллектуальных методов обработки выходных данных [4];

– фаззинг на основе данных об известных ошибках и уязвимостях, в том числе на основе информации открытых баз данных, списков и метрик (*CVE*, *CWE*, *NVD*, *CVSS*, бюллетеней *Microsoft*) [5];

– фаззинг на основе данных о составе и структуре объекта тестирования, включая схемы фаззинга, извлекающие данную информацию из объекта тестирования.

На сегодняшний день существует множество средств анализа веб-приложений: *OWASP ZAP, W9scan, Wapiti, Arachni, Paros, Tenable.io, Burp Suite, Acunetix, XSpider, MaxPatrol,* Сканер-ВС. Данные средства позволяют провести анализ веб-приложений и определить надежность представленного веб-ресурса. Сравнительный анализ представленных средств приведен в таблице.

ТАБЛИЦА. Средства анализа веб-приложений.

Средства анализа	Особенности
OWASP ZAP	Бесплатный Имеется графический интерфейс Локализован на русский язык
W9scan	Бесплатный Консольное средство

Средства анализа	Особенности
Wapiti	Бесплатный Консольное средство
Arachni	Бесплатный Имеется графический интерфейс Обширное поле для настройки тестов
Paros	Бесплатный Имеется графический интерфейс Предустановлен в операционную систему *Kali Linux*
Tenable.io	Платное средство Имеется графический интерфейс Облачная структура сервиса Обширное поле для настройки тестов
Burp Suite	Платное средство Имеется графический интерфейс Обширное поле для настройки тестов
Acunetix	Платное средство Имеется графический интерфейс Обширное поле для настройки тестов
XSpider	Платное средство Имеется графический интерфейс
Сканер-ВС	Платное средство Имеется графический интерфейс

Однако все представленные выше средства имеют общий существенный недостаток. Недостатком является проблема построения структурной модели произвольного веб-ресурса, способная обеспечивать корректировку входных данных. Данный недостаток приводит к появлению ошибок второго рода при проведении тестирования.

Сведения о структуре ПО, как правило, извлекают методами статического анализа исходных текстов, однако современные информационные технологии защиты от анализа ПО веб-приложений эффективность статического анализа исходных текстов сводят к нулю [6]. К таким технологиям относятся шифрования и обфускации исходных текстов [7]. Выходом в данных обстоятельствах является использование динамического анализа [8].

Для фаззинга принципиально важной задачей является формирования эффективной выборки входных данных для тестируемого объекта оценки. При защите клиентского ПО от анализа требуется разработка такого метода исследования, которые позволит активировать все имеющиеся функциональные объекты в составе ПО, передающие удаленной ИС некоторые данные и, по сути, раскрывающие данные о точках входа ПО удаленной ИС.

На сегодняшний день существует множество обфускаторов, применяющих различные способы преобразований. К самым известным относятся:

JSPacker, *JSmin*, *YUI Compressor*, *Google Closure Compiler*, *JJencode*, *JSUnpack*, *WebStorage*, *uglifyjs*2, *JSFuck*, *AAencode*, *URLencode*, *Packer*, *JS Obfuscator*.

Инструменты для деобфускации *JavaScript* кода можно разделить следующим образом:

1. Средства анализа вредоносных программ (*JStillery*, *JSDetox* и др.).
2. Деобфускаторы (*JStillery*, *JSDetoxI*, *JSNice* и др.).
3. Оптимизаторы (*Prepak.io*, *Closure compiler*, *jsbeautifier* и др.).
4. Средства эмуляции *JavaScript* (*Google V8*, *SpiderMonkey*, *Nodejs's VM module* и др.).

Предлагаемый в данной работе подход может быть реализован средствами сценария управления программно-управляемым браузером, функциями которого является моделирование действий пользователя на загруженный в данный браузер *HTML*-странице сайта.

Структурная схема средства анализа веб-приложений на языке *JavaScript*, защищенных методом обфускации представлена на рис.

Исходными данными для средства анализа является *URL* объекта оценки – сайта.

Модуль веб-клиента содержит сценарий на *Python*3, формирующие последовательность событий на загруженной странице. К таким событями могут относиться:

– «клики» по объектам *DOM*-модели *HTML*-страницы;

– движения указателем курсора над объектами DOM-модели *HTML*-страницы;

– инициирование нажатий клавиш клавиуатуры или мыши;

– прокрутка страницы,

а также другие события.

Сценарий веб-клиента содержит команды, формирующие данные события, которые отправляются посредством драйвера *Selenium WebDriver* для веб-браузера.

Драйвер является посредником между сценарием на *Python* и вызываемым веб-браузером.

Поскольку события обрабатывает веб-браузер, то сведения о событиях передаются клиентскому ПО ИС в составе данных *HTML*-страницы.

В случае наличия защищенного от анализа кода на *JavaScript*, инициирующего некий *HTTP*(*s*)-запрос при получении заданных событий, данные этого запроса будут передаваться через компонент веб-браузера, хранящий журнал запросов. Сведения из данного журнала доступны сценарию, моделирующему действия пользователя.

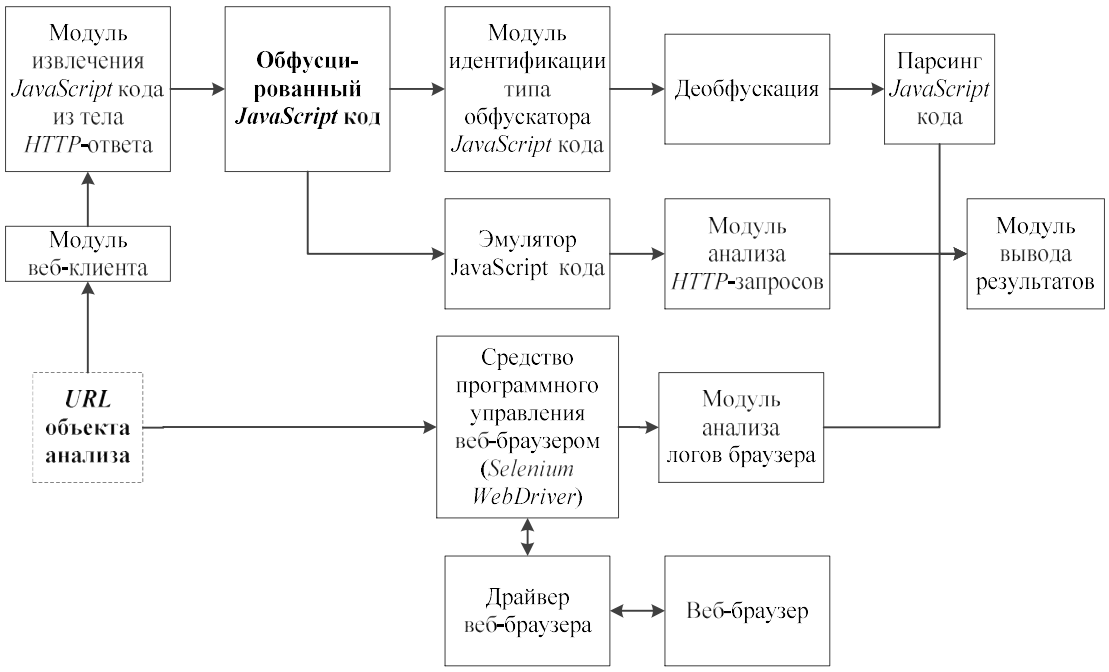


Рис. Схема средства анализа веб-приложений на языке *JavaScript*, защищенных методом обфускации

Таким образом, используя динамический анализ и моделирования действий пользователя, средство анализа позволяет идентифицировать точки входа, используемых удаленной ИС, для получения данных от защищенного от анализа клиентского ПО в составе *HTML*-страницы.

Обобщив полученную информацию о точках входа, средство анализа формирует информационную модель удаленной ИС, которая, в свою очередь, позволит более эффективно подготовить исходные данные для ее фаззинга.

Список используемых источников

1. Российская Федерация. Законы. О безопасности критической информационной инфраструктуры Российской Федерации : федер. закон от 26.07.2017 № 187-ФЗ : [принят Гос. Думой 12 июля 2017 г. : одобр. Советом Федерации 19 июля 2017 г.] // Официальный интернет-портал правовой информации : сайт. в ред. Федерального закона от 03.08.2018 № 323-ФЗ. Электрон. дан. 2005–2020. URL: http://publication.pravo.gov.ru/Document/Text/0001201707060023 (дата обращения 28.11.2020).

2. Марков А. С., Цирлов В. Л., Барабанов А. В. Методы оценки несоответствия средств защиты информации / под ред. доц. А. С. Маркова. М.: Радио и связь, 2012. 192 с.

3. Маркин Д. О., Зверев А. А. Адаптивный фаззинг веб-приложений на основе модели веб-ресурса // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019): VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2019. Т. 2. 603 с. С. 288–293.

4. Котенко И. В., Степашкин Е. В., Дойникова Е. В. Анализ защищенности автоматизированных систем с учетом социо-инженерных атак // Проблемы информационной безопасности. Компьютерные системы. Москва, 2011. № 3. С. 40–57.

5. Полухин П. В. Байесовские модели и алгоритмы управления процессом тестирования веб-приложений методом фаззинга: дис. … канд. техн. наук: 05.13.18. Воронеж, 2016. 180 с.

6. Маркин Д. О., Зверев А. А., Саклаков А. И., Рыков Д. А. Технологии распознавания моделей точек входа веб-приложений // Безопасные информационные технологии : Десятая международная научно-техническая конференция : сб. трудов (Москва, 3–4 декабря, 2019 г.). Москва : МГТУ им. Н.Э. Баумана, 2019. 409 с. : ил. С. 275–280.

7. Варнавский Н. П., Захаров В. А., Кузюрин Н. Н., Шокуров А. В. Современное состояние исследований в области обфускации программ: определение стойкости обфускации // Труды ИСП РАН. Т. 26. Вып. 3. 2014. С. 167–198. doi: 10.15514/ISPRAS-2014-26(3)-9.

8. Маркин Д. О., Зверев А. А., Макеев С. М. Алгоритм распознавания точек входа обфусцированных веб-приложений методом динамического анализа // Известия Тульского государственного университета. Технические науки. 2020. Вып. 9. С. 28–40.

УДК 004.056.5
ГРНТИ 50.37.23

АВТОМАТИЗАЦИЯ СОЗДАНИЯ УЗЛА РАСПРЕДЕЛЕННОЙ СЕТИ НА ОСНОВЕ ТЕХНОЛОГИИ *SELENIUM WEBDRIVER*

Д. О. Маркин, А. В. Щукин

Академия Федеральной службы охраны Российской Федерации

В статье приводится описание принципов построения распределенных вычислительных сетей, анализ их достоинств. Разобран пример реализации автоматизированного процесса создания узла распределенной вычислительной сети при помощи инструмента тестирования веб-приложений Selenium WebDriver и языка программирования высокого уровня python.

распределенная вычислительная сеть, Selenium, Selenium WebDriver, python, P2P.

Введение

Трудоемкие вычислительные задачи требуют от современных компьютеров высокой мощности процессоров и обеспечения процесса распараллеливания ресурсов машины. Однако все чаще инженеры приходят к мысли создания сети, каждый узел которой будет заниматься выполнением небольшой задачи, совокупность которых представляет исходную. На этом принципе построены распределенные вычислительные системы (РВС) [1].

Концептуальным преимуществом таких систем является способность выполнять параллельные вычисления, за счет чего в системе может быть достигнута производительность, превышающая максимально возможную на данный момент производительность отдельного процессора.

Другое важное достоинство распределенных систем – это их принципиально более высокая отказоустойчивость. Она базируется на избыточности. Избыточность обрабатывающих узлов (компьютеров в сетях) позволяет при отказе одного узла переназначать его задачу другим компьютерам сети. С этой целью в распределенной системе могут быть предусмотрены процедуры динамической или статической реконфигурации. Также предусмотрена возможность дублирования данных на несколько компьютеров сети, так что при отказе одного из них данные остаются доступными.

Несмотря на то, что каждый вычислительный узел распределенной сети является автономным, программная составляющая РВС [1] должна обеспечивать пользователям видимость работы с единой вычислительной системой. В связи с этим выделяют следующие важные характеристики РВС:

– возможность работать с различными типами устройств;

– возможность простого расширения и масштабирования;

– перманентная доступность ресурсов;

– сокрытие особенностей коммуникации от пользователей.

Для обеспечения функционирования РВС в виде единого целого, стек программного обеспечения (ПО) разбивают на два слоя. На верхнем слое располагаются распределенные приложения, отвечающие за решение определенных прикладных задач средствами РВС. Их функциональные возможности базируются на нижнем слое – промежуточном программном обеспечении (ППО). ППО взаимодействует с системным ПО и сетевым уровнем, для обеспечения прозрачности работы приложений в РВС.

Рис. Слои программного обеспечения в РВС

Создание узла распределенной сети на основе технологии Selenium Webdriver

Selenium – это открытый и портативный инструмент для автоматизации тестирования веб-приложений [2, 3]. *Selenium* – это не просто инструмент, а набор инструментов, одним из которых является *Selenium WebDriver*, кото-

рый представляет собой программную библиотеку для управления различными браузерами. Ниже приведено пошаговое описание создания узла распределенной сети с использованием *Selenium WebDriver* и языка программирования высокого уровня *python* 3.

Первоначально необходимо установить библиотеку для работы с *WebDriver* командой pip install selenium. Далее необходимо загрузить драйвер для работы с определенным браузером. В данной работе будет описана работа с браузером Mozilla Firefox, поэтому необходимо установить драйвер geckodriver.exe. После чего в самом проекте подключить необходимые для разработки библиотеки:

```
from selenium import webdriver
import time
from selenium.webdriver.common.keys import Keys
from selenium.webdriver.common.by import By
from selenium.webdriver.support.ui import WebDriverWait
from selenium.webdriver.support import expected_conditions as EC
import keyboard
```

Для работы с определенным хостинг-провайдером разработан класс, полями которого выступают объект класса *webdriver,* который отвечает за выполнение команд в браузере*, url* хост-провайдера, который предоставит возможность создания узла, адрес и пароль электронной почты, используемой для регистрации пользователя.

```
class reg_000w(object):
    def __init__(self, browser, url, mail, passwd):
        self.browser = browser
        self.url = url
        self.mail = mail
        self.passwd = passwd
```

В главной функции выполнено создание объекта драйвера браузера Firefox и задание опций, которые предотвращают распознавание автоматического управления браузером, а также выполнения ряда функций, работа которых рассмотрена ниже.

```
def main():
    option = webdriver.FirefoxOptions()
    option.set_preference('dom.webdriver.enabled', False)
    driver = webdriver.Firefox(options=option)
```

```
bot = reg_000w(driver, "https://ru.000webhost.com/besplatnaya-registraciya", "your-email@gmail.com", "yourpassword")
bot.registration()
bot.mail_confirm()
bot.tear_down()
```

Функция registration() выполняет загрузку веб-страницы регистрации хостинг-провайдера и осуществляет ввод регистрационных данных нового пользователя.

```
def registration(self):
    self.get_url()
    self.input_data()
def get_url(self):
    self.browser.get(self.url)
    time.sleep(5)
def input_data(self):
    email = self.browser.find_element_by_css_selector("#cpanel-signup-email")
    email.send_keys("your-email@gmail.com @gmail.com")
    passwd = self.browser.find_element_by_css_selector("#cpanel-signup-password")
    passwd.send_keys("yourpassword ")
    passwd_repeat = self.browser.find_element_by_css_selector("#cpanel-signup-repeat-password")
    passwd_repeat.send_keys("yourpassword ")
    registration = self.browser.find_element_by_css_selector("button.button--primary")
    registration.click()
    time.sleep(5)
```

После ввода данных необходимо подтвердить регистрацию в электронной почте. Ниже приведенная функция осуществляет вход в почту пользователя, поиск письма от хостинг-провайдера и процедуру подтверждения регистрации.

```
def mail_confirm(self):
self.browser.get("https://accounts.google.com/signin/v2/identifier?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&service=mail&sacu=1&rip=1&flowName=GlifWebSignIn&flowEntry=ServiceLogin")
```

```
    login = self.browser.find_element_by_css_selector("#identifierId")
    login.send_keys("your-email@gmail.com")
    next = self.browser.find_element_by_css_selector("div.VfPpkd-RLmnJb")
    next.click()
    time.sleep(3)
    self.browser.implicitly_wait(5)
    password = self.browser.find_element_by_css_selector("[name='pass-
word']")
    password.click()
    password.send_keys("yourpassword")
    next = self.browser.find_element_by_css_selector("div#passwordNext
div.VfPpkd-RLmnJb")
    next.click()
    time.sleep(3)
    link = 0
    letter_links = self.browser.find_elements_by_css_selector("div.yW
span.bA4 span")
    for letter_link in letter_links:
       if letter_link.get_attribute('name') == "000webhost.com":
          letter_link.click()
          break
    confirm = self.browser.find_element_by_css_selector("table[align='center']
tbody tr td[align='center'] a")
    confirm_href = confirm.get_attribute('href')
    self.browser.get(confirm_href)
    time.sleep(5)
```

После подтверждения регистрации необходимо ввести имя проекта и пароль для доступа к нему. Затем перейти в файловый менеджер хостинга, куда необходимо добавить скрипты, например с использованием протокола передачи файлов *FTP* в языке *pyhon* библиотека *ftplib*, которые будут организовывать взаимодействие между узлами распределенной вычислительной сети.

Выводы

Технология *Selenium WebDriver* позволяет производить автоматизацию процесса создания одноранговой сети, в которой в качестве узлов могут выступать вычислительные машины, предоставленные различными провайдерами услуг хостинга. Таким образом, можно обеспечить развертывание устойчивой РВС, для дальнейшего решения прикладных задач, в короткие сроки.

Список используемых источников

1. Радченко Г. И. Распределенные вычислительные системы : учеб. пособие. М., 2012. С. 8–12.
2. Avasarala, S. Selenium WebDriver Practical Guide. PACKT publishing, 2012.
3. Burns, D. Selenium 1.0 Testing Tools: Begginers Guide. PACKT publishing, 2010.

УДК 621.391
ГРНТИ 49.27.31

АНАЛИЗ СОСТОЯНИЯ И ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ МОДЕМОВ ПЕРЕДАЧИ ДАННЫХ ДКМВ ДИАПАЗОНА

М. Л. Маслаков

АО «Российский институт мощного радиостроения»

В работе представлен анализ существующих модемов передачи данных ДКМВ диапазона. Выделены некоторые актуальные задачи для дальней ДКМВ связи. Показаны направления развития и совершенствования моделей, сигнально-кодовых конструкций и алгоритмов их обработки, для повышения вероятностно-временных показателей радиолинии.

модем передачи данных, ДКМВ диапазон, адаптивная связь.

Для обеспечения оперативного информационного обмена различными видами сообщений между абонентами, минуя каналы и линии сетей связи общего пользования, важнейшее значение имеет декаметровый диапазон волн (ДКМВ). Технический потенциал, высокая мобильность и относительная дешевизна приемо-передающего оборудования, а также роль ДКМВ диапазона как стратегического резерва, сохраняют актуальность и необходимость совершенствования средств ДКМВ радиосвязи [1].

Возможность передачи сообщений на дальние расстояния, в том числе за пределы прямой видимости, учитывая обширность территории Российской Федерации, а также активное освоение Арктической зоны [2], отводит важную роль ДКМВ радиосвязи для решения разнообразных задач в интересах различных служб и ведомств (северный морской путь, гражданская авиация).

При этом, ДКМВ диапазон характеризуется нестационарностью характеристик радиоканала и многолучевым распространением, что проявляется как частотно-селективные замирания. Поэтому современные модемы ДКМВ связи и передачи данных представляют собой системы с многопараметрической адаптацией [2], основная сложность реализации которых связана с решением комплекса задач цифровой обработки сигналов, таких как: оценка и прогноз характеристик радиоканала; применение методов адаптивной фильтрации и коррекции; выбор оптимальных сигнально-кодовых конструкций, исходя из условий распространения.

Отметим, что если 10–20 лет назад актуальности совершенствования и модернизации ДКМВ модемов, в основном, способствовало бурное развитие вычислительной техники (что позволило реализовать более сложные алгоритмы), то последние 5 лет этому способствуют новые специфические задачи [3, 4] и повышающиеся требования к вероятностно-временным характеристикам доведения сообщений.

В частности к таким задачам можно отнести передачу формализованных сообщений [5] за заданное время с достаточно высокой вероятностью доведения. Не менее важной задачей является организация полносвязной радиосети. При этом всегда остается актуальной задача повышения информационной скорости передачи данных.

Для организации ДКМВ радиолинии типа «борт-земля» применяют модемы с полосой порядка 3 кГц, одночастотного типа эффективно использующие мощность передатчика [5]. Также такие модемы устойчивы к влиянию допплеровского смещения частоты, и поэтому их применяют, в частности, для организации ДКМВ радиоканала в авиации. Известны следующие одночастотные модемы, реализованные в соответствии с зарубежными стандартами ARINC 635 [6], MIL-STD-110C [7], STANAG-4539 [8], STANAG-4285 [9]. Однако применение таких модемов требует значительных затрат на передачу тестовых сигналов, что снижает информационную скорость.

Для обеспечения более высокой скорости передачи применяют модемы, использующие OFDM сигналы [10]. Такие модемы эффективней используют выделенную полосу спектра, однако обладают рядом недостатков, таких как значительный пик-фактор, что снижает энергетические характеристики радиолинии, а также наличие побочных излучений из-за нелинейности выходных трактов передатчика.

Помехоустойчивость OFDM-модемов несколько выше, и они потенциально позволяют обеспечить большую скорость передачи данных, однако в каналах с высокой скоростью и селективностью замираний, обусловленными большой возмущенностью ионосферы, одночастотные модемы значительно превосходят многочастотные по помехоустойчивости. Поэтому в модеме MIL-STD-110C сочетается применение обеих указанных технологий,

что позволяет получать наиболее высокие показатели производительности при ведении адаптивной радиосвязи.

Вместе с тем современные требования к системам связи, часто, характеризуются повышением скорости передачи данных. Основным направлением решения указанной задачи является увеличение ширины полосы сигнала. В настоящее время известны комплексы ДКМВ связи? использующие полосу 6 кГц (верхняя и нижняя боковые полосы) [1], а также использование сигналов в полосе частот от 12 кГц до 24 кГц, что позволяет потенциально говорить о скоростях более 70 кбит/с.

Однако важно отметить, что далеко не всегда имеется возможность использования такой полосы на реальных радиотрассах. Поэтому, важным направлением развития является анализ характеристик радиоканала и прогноз. Кроме того, использование таких сигналов повышает требования к линейности радиопередающих трактов.

Для работы в сложных условиях со значительным многолучевым распространением требуется сочетание учета специфики (физики) распространения радиоволн и современных методов цифровой обработки сигналов. Большой потенциал при этом имеют итеративные алгоритмы обнаружения, обработки и декодирования сигнально-кодовых конструкций (СКК). Итеративные адаптивные алгоритмы позволяют достичь потенциального оптимума выбранной целевой функции [11]. Дополнительно высокую производительность обеспечивают применение методов мягкого декодирования, использования кодов с малой проверкой на четность (LDPC, F-LDPC) [12, 13] и итеративной реализации декодера [14]. Решение этой задачи, в том числе, связано с решением задачи статистического анализа символов и/или бит на выходе демодулятора.

В тоже время выбор СКК связан со спецификой передаваемой информации и требованиям к выдаче ее абоненту. В частности, при передаче файлов не допускается наличие ошибок, напротив, при передаче текстовых сообщений иногда допускается некоторая доля ошибок («опечаток»). Это накладывает требования к исправляющей способности СКК и, как следствие, к потенциальной избыточности и скорости передачи.

Однако при применении сигналов в широкой полосе требует внимания одна задача, а именно используемая модель ДКМВ канала. Для анализа характеристик ДКМВ модемов по настоящее время широко используется для тестирования модемов модель Ваттерсона [15], предложенная в 1969 году. Модель позволяет сопоставить характеристики различных модемов в условиях нескольких лучей с независимыми релеевскими замираниями в соответствии с рекомендациями ITU-R F.520 [16]. Отмечается, что хотя имитаторы, реализующие эту модель, далеки от поведения реального канала, характеристики модемов, полученные на модели Ваттерсона, близки к характеристикам, полученным в реальных каналах, поэтому данный имитатор

используется по настоящее время для тестирования современных КВ модемов.

Однако модель Ваттерсона обладает двумя существенными ограничениями: во-первых, она была разработана и протестирована для полосы канала не более 12 кГц; во-вторых, модель предполагается стационарной, что может иметь место для периода времени не более 10 минут. Кроме того, отсутствует возможность моделирования КВ сетей.

Таким образом, одним из направлений развития можно указать разработку имитатора КВ канала. Отметим, что предложены несколько моделей, отличающиеся широкополосностью и большей реалистичностью к реальному каналу, в которых частично снимаются указанные выше ограничения. Это модель Воглера-Хофмейера [17, 18] и псевдо-детерминированная модель [19]. Однако сведения о их практическом применении для анализа вероятностных характеристик модемов и комплексов связи автору неизвестны.

Таким образом, достижение современных показателей эффективности ДКМВ комплексов передачи данных сочетает решение ряда, на первый взгляд, несвязанных задач, а также учет специфики передаваемых данных и требований надежности. При этом перспективным является применение итерационных алгоритмов обработки СКК, как в части адаптивной фильтрации, так и декодирования.

Список используемых источников

1. Березовский В. А., Дулькейт В. А., Савицкий О. К. Современная декаметровая радиосвязь. М.: Радиотехника, 2011. 444 с.

2. Ступницкий М. М., Лучин Д. В. Потенциал КВ-радиосвязи – для создания цифровой экосистемы России // Электросвязь. 2018. № 5. С. 49–54.

3. Дотолев В. Г., Лашкевич А. В. Цифровое звуковое радиовещание. Состояние и перспективы // Электросвязь. 2019. № 9. С. 14–21.

4. Лучин Д. В., Гавлиевский С. Л., Маслов Е. Н. Масштабируемая телематическая система для арктических регионов РФ с использованием КВ-радиосвязи // Электросвязь. 2019. № 9. С. 22–31.

5. Johnson, E. E.; Koski, E.; Furman, W. N.; Jorgenson, M.; Nieto. J. Third-Generation and Wideband HF Radio Communications. Artech House, Inc, Boston, 2013. 250 p.

6. ARINC Characteristic 635-4. HF Data Link Protocol. Dec. 1, 2003.

7. MIL-STD-188-110C. Interoperability and Performance Standards for Data Modems. Sept. 23, 2011.

8. STANAG 4539. Technical Standards for Non-hopping HF Communications Waveforms. Sept. 15, 2003.

9. STANAG 4285. Characteristics of 1200/2400/3600 Bits per Second Single Tone Modulators/Demodulators for HF Radio Links. Feb. 9, 1993.

10. Бакулин М. Г., Крейнделин В. Б., Шлома А. М., Шумов А. П. Технология OFDM. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2016. 352 с.

11. Джиган В. И. Адаптивная фильтрация сигналов: теория и алгоритмы. М.: Техносфера, 2013.

12. Halford, T. R.; Bayram, M.; Kose, C.; Chugg, K. M.; Polydoros, A. The F-LDPC Family: High-Performance Flexible Modern Codes for Flexible Radio // 2008 IEEE 10th International Symposium on Spread Spectrum Techniques and Applications, Bologna, Italy, 2008. Pp. 376–380.

13. Tomlinson, M.; Tjhai, C. J.; Ambroze, M. A.; Ahmed, M.; Jibril, M. Error-Correction Coding and Decoding. Cham: Springer, 2017.

14. Золотарев В. В., Зубарев Ю. Б., Овечкин Г. В. Многопороговые декодеры и оптимизационная теория кодирования. М.: Горячая линия–Телеком, 2012.

15. Watteson C. C., Juroshek J. R., Bensema W. D. Experimental Confirmation of an HF Channel Model // IEEE Transactions on Communication Technology. 1970. Vol. COM-18. № 6. Pp. 792–803.

16. Recommendation ITU-R 520-2. Use of High Frequency Ionospheric Channel Simulators. 1992. 4 p.

17. Vogler, L. E.; Hoffmeyer, J. A. A model for wideband HF propagation channels // Radio Science. 1993. Vol. 28. № 6. Pp. 1131–1142.

18. Vogler, L. E.; Hoffmeyer, J. A. A New Approach to HF Channel Modeling and Simulation Part II: Stochastic Model // U.S. Department of Commerce. NTIA Report 90–255. 1990. February. 37 p.

19. Le Roux, Y. M.; Niberon, M.; Fleury, R.; Menard, J.; Jolivet, J. P. HF Channel Modelling and Simulation // 5th International Conference on Radio Receivers and Associated Systems. London, 1990. Pp. 72–76.

УДК 004.514
ГРНТИ 81.95.61

РАССМОТРЕНИЕ КОНЦЕПТУАЛЬНЫХ ПРИНЦИПОВ ИСПОЛЬЗОВАНИЯ АНИМАЦИИ ПРИ ПРОЕКТИРОВАНИИ ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА

С. В. Махортов, И. С. Пузанов, А. В. Фёдорова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Использование анимации в настоящее время является трендом в разработке интерфейсов различных программных продуктов. Многие средства проектирования интерфейсов предлагают широкий спектр возможностей по реализации этих функций. Но необходимость использования анимационных спецэффектов в интерфейсах программных продуктов приводит к дополнительным временным и финансовым затратам, не обусловленным практической пользой для функционирования программного обеспечения. В статье рассматриваются виды анимации, применяемые в программах, анализируются проблемы, возникающие при избыточном использовании анимации и возникающие при этом последствия. Делаются соответствующие выводы.

анимация, функциональная анимация, эмоциональная анимация, проектирование пользовательского интерфейса.

Проектирование интерфейса мобильных приложений консолидирует множество аспектов разрабатываемого программного обеспечения, от целевой аудитории до среды его распространения. В основе каждого приложения лежит его функциональность, которая определяется его предназначением для той или иной категории пользователей. Наряду с этим, дизайнеры и разработчики программного продукта задумываются о пользовательском опыте при взаимодействии с интерфейсом, рассматривая как способ донесения информации и функционала приложения до пользователя, анимацию. Однако повсеместное использование анимации не всегда целесообразно с финансовой и временной стороны при разработке программного продукта [3].

Анимацию визуальных элементов программного обеспечения можно разделить на две категории: функциональная и эмоциональная [2]. Классификационная схема показана на рис. 1.

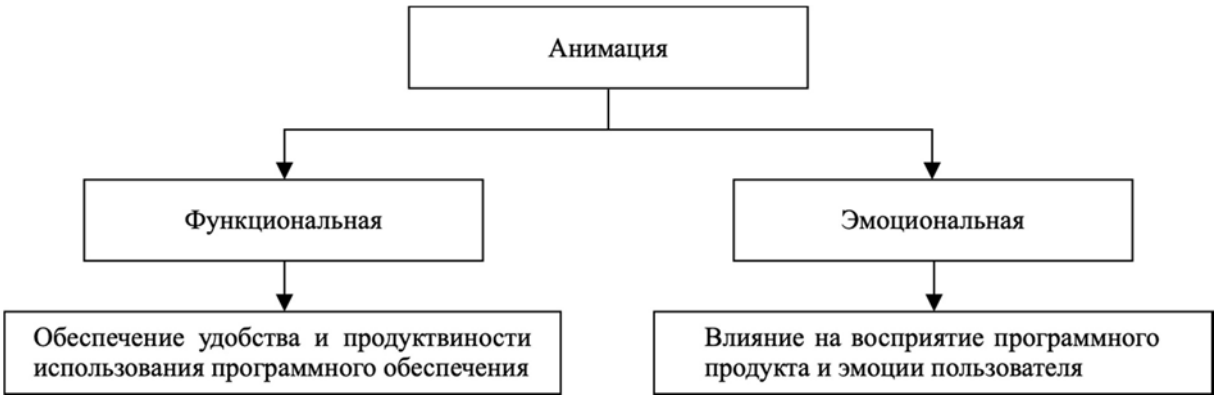


Рис. 1. Классификация анимации по назначению

Рассмотрим эти два вида анимации более подробно.

Функциональная анимация

При проектировании функциональной анимации, перед дизайнерами и разработчиками ставится задача донести до пользователя историю о том, как работает приложение, что происходит в момент взаимодействия с визуальными элементами. Основой правильного проектирования функциональной анимации является реализация следующих обработок событий:

– обратная связь анимации,
– ориентация в пространстве,
– помощь пользователю.

Обратная связь анимации.

Задача этого функционала заключается в том, чтобы дать пользователю понять, что произошло какое-то событие, и помочь ему взаимодействовать с интерфейсом, как если бы это был реальный физический объект. Однако в дизайне анимации мобильных приложений, анимация обратной связи должна создать естественное чувство физики, которое будет единообразно во всем приложении.

Ориентация в пространстве.

Пользовательские интерфейсы зачастую основаны на статических дисплеях – серии дисплеев, каждое из которых показывает новое состояние системы. Изменения состояния в таких пользовательских интерфейсах по умолчанию связаны с резкими сокращениями, из-за чего за ними трудно уследить. В когнитивной науке это называется «слепота невнимания» – когда внезапные изменения не позволяют пользователям замечать новую информацию. Если визуальные изменения в интерфейсе происходят внезапно, пользователи могут потерять понимание интерфейса [1].

Помощь пользователю

Анимация позволяет показать пользователю, как взаимодействовать с интерфейсом. Если приложение имеет сложную структуру, необходимо с самого первого запуска объяснить пользователю, как приложение работает.

Эмоциональная анимация

Функциональная анимация обеспечивает удобство и продуктивность использования программного обеспечения, в то время как эмоциональная анимация влияет на чувства пользователей.

Изобилие мобильных программных продуктов задает ощущение единообразия пользовательских интерфейсов, и потому ключевую роль играет анимация: пользователи замечают детали. Сосредоточение внимания на эмоциях пользователя играет огромную роль во взаимодействии с пользовательским интерфейсом. *Aarron Walter* в книге «*Design for emotions*» декларирует следующее: «Личность – это таинственная сила, которая привлекает нас к одним людям и отталкивает от других», следовательно и интерфейсу должна быть присуща человечность, поощряя пользователя анимационными эффектами при достижении личных целей.

Лучшая анимация та, которая кажется естественной и не привлекает к себе слишком много внимания. *Michaël Villar* предлагает следующий метод тестирования анимации: «Если отключить всю анимацию, поток будет казаться нарушенным, в противном случае это может означать, что анимации излишни».

Эмоциональная анимация проектируется простой и рассчитанной на многократное использование. Грамотно спроектированная эмоциональная анимация превращает программный продукт из последовательности

статических экранов в спланированный динамический опыт, который заставит пользователей возвращаться к приложению вновь [1].

Заключение

Рассмотрев две основные категории анимационных эффектов визуальных элементов в интерфейсах мобильных приложений, сопоставив цели и задачи каждой из них, стоит выделить следующее:

1. Анимация является элементом дизайна, обеспечивая восприятие того, как программное обеспечение функционирует и какую задачу оно выполняет.

2. Следуя принципам функциональной анимации, дизайнеры и разработчики программного продукта гарантируют пользователям правильный опыт взаимодействия с интерфейсом и решения поставленных перед приложением задач.

3. Эмоциональная анимация является опциональным решением при разработке программного продукта. Целью данной анимации является привлечение внимания пользователя к продукту.

4. Решение об использовании анимации в приложении целесообразно тогда, когда она несет смысловую нагрузку и не отвлекает пользователя от выполнения основных задач.

Список используемых источников

1. Babich, Nick. Using Animation to Improve the Mobile App User Experience. URL: https://www.shopify.com/partners/blog/using-animation-to-improve-mobile-app-user-experience (дата обращения 20.03.2021).

2. How to Effectively Incorporate Animation in Your Mobile App Design. URL: https://protoio.medium.com/how-to-effectively-incorporate-animation-in-your-mobile-app-design-439d2945dbf0 (дата обращения 20.03.2021).

3. Zakurdaieva, Alyona; Osadchiy, Victor. How to create mobile UI animations that meet user’s need. URL: https://yalantis.com/blog/how-to-create-mobile-ui-animations-that-meet-users-needs/ (дата обращения 20.03.2021).

УДК 004.89
ГРНТИ 81.93.29; 20.53.19

О МЕТОДЕ ДИФФЕРЕНЦИАЦИИ КОНФИДЕНЦИАЛЬНЫХ СВЕДЕНИЙ В ИНФОРМАЦИОННЫХ ПРОЦЕССАХ ПРИ ВЗАИМОДЕЙСТВИИ ГИС

А. Н. Метельков

Санкт-Петербургский университет ГПС МЧС России

Успешность деятельности руководителей ликвидации чрезвычайных ситуаций по выработке управленческих решений зависит от их осведомленности, основанной на взаимодействии информационных систем. Эффективность взаимодействия информационных систем определяется организацией обмена данными, командами и сигналами, предусматривающей дифференциацию конфиденциальных сведений в информационных процессах.

конфиденциальность, сведения, информационные процессы, информационный обмен, дифференциация.

Изменения в государственном секторе связаны с внедрением современных информационно-коммуникационных технологий, применение которых в работе органов государственной власти рассматривается как главный потенциал роста эффективности государственного управления [1].

Требования нормативных правовых актов и государственных регуляторов Роскомнадзора, ФСБ, и ФСТЭК России направлены на обеспечение конфиденциальности, целостности, доступности, неотказуемости информации при ее хранении и передаче.

Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Нередко эти требования являются непреодолимым препятствием для налаживания и согласования информационного обмена при различном статусе конфиденциальной информации. Исторически сложилась и получает дальнейшее развитие ведомственная дифференциация требований к защищённой передаче служебной информации, обусловленная международными и отечественными нормативными правовыми актами и руководящими документами регуляторов.

Рассмотрим актуальность предлагаемого метода реализации обмена конфиденциальными данными на основе их дифференциации. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является требование о соблюдении конфиденциальности информации, доступ к которой ограничен федеральными законами.

Государственные информационные системы (ГИС) создаются для реализации полномочий государственных органов и обеспечения обмена между ними разноплановой информацией, а также в иных установленных федеральными законами целях. Такие системы создаются и эксплуатируются на основе документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.

Среди главных причин, обусловливающих актуальность дифференциации обмена конфиденциальной информацией в рамках взаимодействия, ГИС систем можно выделить следующие:

– прямая связь информационного обмена с разрешением конкретных практических задач государственного управления;

– требования целого ряда регулирующих документов организационно-правового характера;

– необходимость обеспечения защиты служебной информации ограниченного распространения при информационном взаимодействии.

Дифференцированный обмен конфиденциальной информацией делает систему государственного управления более гибкой и эффективной, что создает условия для совершенствования механизмов доступа лиц к процессу принятия управленческих решений. Совершенствование новых технологий приводят к росту степени вовлеченности субъектов взаимодействия в процессе подготовки и принятия таких решений, обеспечивая необходимую прозрачность информационных процессов в условиях соблюдения требований к защите конфиденциальности, целостности и доступности информации ограниченного распространения.

В рассматриваемом контексте показателен пример МЧС России, которое и его территориальные органы являются постоянно действующими органами управления Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС) соответственно на федеральном, межрегиональном и региональном уровнях и интегрирует информационные и иные ресурсы большинства министерств и ведомств.

На повышения эффективности РСЧС к действиям по предназначению являются вопросы цифровой трансформации МЧС России. Поэтому дифференциацию конфиденциальной информации рассмотрим на примере МЧС,

которое выполняет важнейшую государственную задачу – защиту людей и территорий от чрезвычайных ситуаций. В 2020 году благодаря использованию цифровых технологий, а также своевременно принятым мерам, минимизированы издержки на ликвидацию последствий чрезвычайных ситуаций и компенсационные выплаты.

22 декабря 2020 г. во время визита в Национальный центр управления в кризисных ситуациях МЧС глава Правительства РФ поручил МЧС России создать единую базу ведомственных и региональных данных ресурсов для их оперативного привлечения в случае чрезвычайных ситуаций. Национальный центр управления в кризисных ситуациях МЧС России – орган повседневного управления РСЧС. В центре работают специалисты в области оповещения и информирования населения, оперативного реагирования, моделирования, мониторинга и анализа чрезвычайных ситуаций, IT-технологий, космического мониторинга, обеспечения связи и психологи. ГУ НЦУКС и центры управления в кризисных ситуациях территориальных органов МЧС России выполняют задачи системы антикризисного управления при возникновении чрезвычайных ситуаций. На базе НЦ действует АИУС РСЧС-2030. Руководство МЧС сообщило главе правительства о том, что ряд министерств и ведомств подключились к этой базе. Однако необходима поддержка для обеспечения возможности подключения к информационным ресурсам других министерств, чтобы ведомственная программа искусственного интеллекта сама бы отбирала информацию, необходимую для решения задач. Глава правительства пообещал оказать содействие в том, чтобы все федеральные министерства и ведомства направили такую информацию в создаваемое спасателями «озеро данных» по разработанному МЧС алгоритму [2].

Для того, чтобы отдельные категории данных «не утонули» и «не растворились» в этом «озере» необходима дифференциация информации. При этом следует учитывать возможную трансформацию информации из одной группы в другую с соблюдением некоторых ограничительных требований, как например, в случае с персональными данными. В основе предлагаемого метода дифференциации конфиденциальной информации лежит ее разделение на пять больших групп.

Критерием является субъектный признак конфиденциальной информации:

– персональные данные;

– собственная ведомственная служебная информация ограниченного распространения;

– служебная информация сторонних государственных органов и организаций, государственных корпораций;

– служебная информация органов местного самоуправления;

– служебная информация других организаций;

– общедоступная служебная информация.

Такой метод позволяет алгоритмизировать и осуществлять машинную обработку информации, обеспечивая отдельные особенности ее защиты для соблюдения ведомственных и корпоративных интересов.

Список используемых источников

1. Булгатова Ю. С., Дырхеев А. В. Информационные технологии как средство модернизации государственного управления в современном обществе // Вестник БГУ. Экономика и менеджмент. 2018. № 1. С.8–15.

2. Михаил Мишустин посетил Национальный центр управления в кризисных ситуациях МЧС России // URL: http://government.ru/news/41190/ (дата обращения 21.02.2021)

УДК 621.396.4
ГРНТИ 50.37.03

ФОРМУЛИРОВКА ЭТАПОВ И ОСОБЕННОСТЕЙ РАЗРАБОТКИ МЕТОДИКИ ОЦЕНИВАНИЯ НАДЕЖНОСТИ СОВРЕМЕННЫХ МОБИЛЬНЫХ ДАТА-ЦЕНТРОВ

А. В. Михайличенко, Н. В. Михайличенко, И. Б. Паращук

Военная академия связи

Проведен анализ научно-практических подходов к совершенствованию методологии и инструментария оценивания надежности современных мобильных дата-центров. Основное содержание статьи составляет формулировка задач и детальное описание этапов разработки методики многокритериального оценивания надежности мобильных дата-центров в различных условиях обстановки, с учетом различных аспектов неопределенности исходных данных, которые могут быть учтены в рамках математики гранулированных (гранулярных) вычислений.

мобильный дата-центр, оценивание, обработка данных, надежность, методика, система, показатель, отказоустойчивость, этап.

Развитие современного информационного общества невозможно без эволюционных (либо, иногда, революционных) шагов в рамках развития IT-инфраструктуры этого общества. Это касается как всех секторов экономики, сферы здравоохранения, так и оборонной сферы и сферы обеспечения безопасности. Очевидно, что для реализации своевременного и эффективного управления всеми сферами жизни страны и общества необходимо использовать новейшую IT-инфраструктуру, и эти вопросы уже успешно решаются

в России [1]. Ключевым элементом построения IT-инфраструктуры практически любого масштаба являются дата-центры [2]. В большинстве случаев под дата-центром понимается специализированное помещение (стационарное сооружение или мобильное помещение) для размещения (хостинга) серверного и сетевого оборудования. С помощью этого оборудования к дата-центрам подключаются абоненты по каналам специализированных сетей или глобальной сети Интернет.

Вместе с тем, особое внимание специалистов в последние годы сосредоточено на поиске новых технических и программных решений по хранению и обработке больших массивов данных. Это связано с тем, что в течение жизненного цикла современного дата-центра, по некоторым данным, сменяется от трех до пяти поколений серверного и сетевого оборудования, а объем данных удваивается каждые восемнадцать месяцев [3]. В этих условиях все более очевидна необходимость разработки гибких и масштабируемых систем хранения данных. Эффективным решением данных проблем могут стать мобильные дата-центры (МДЦ) [4].

Неоспоримыми преимуществами МДЦ, к которым также относят контейнерные и модульные дата-центры, являются удобство их транспортировки и возможность работы в любой местности. Мобильный дата-центр – одномодульный центр обработки данных, который размещен либо в специальном боксе (кунге – кузове универсальном нормального габарита) на транспортной базе (грузовой автомобиль, судно, самолет), либо в специализированном транспортном контейнере (может перевозиться железнодорожным или водным транспортом). Он, как и его стационарный аналог, оснащен комплексом информационной, телекоммуникационной и инженерной инфраструктуры, подключен к каналам связи и предназначен для хранения и обработки информации, а также для оказания широкого диапазона иных услуг, которые может предоставить хранилище данных.

При этом контейнерный дата-центр – самый распространенный тип МДЦ с готовой инфраструктурой для размещения серверов, систем хранения данных и другого IT-оборудования. Это либо одиночный контейнер или набор контейнеров со всеми компонентами дата-центра: серверными стойками, коммуникациями, системами электропитания и охлаждения.

Классический МДЦ обычно смонтирован на базе большегрузного автомобиля с размещенным внутри комплексом информационной, телекоммуникационной и инженерной инфраструктуры. Типовой МДЦ представляет собой небольшой автономный и готовый к эксплуатации автомобильный модуль, который внутри оборудован серверными стойками, структурированной кабельной системой, системами бесперебойного и гарантированного электропитания, системами вентиляции и кондиционирования, средствами противопожарной защиты и средствами контроля управления доступа, мониторинга и управления инфраструктурой [5].

Мобильные дата-центры предназначены для: оперативного развертывания IT-инфраструктуры в труднодоступных и, зачастую, отдаленных местах; для «приближения к клиенту» – размещения IT-инфраструктуры рядом с потребителями; для реализации возможности частого перемещения (перевозки) и установки в различных местах; для быстрого развертывания инфраструктуры или увеличения ее мощности (масштабирование), а также для выполнения функций резервного дата-центра [6].

Применение МДЦ позволить снизить количество функциональных узлов (аппаратных, серверных, кроссовых), унифицировать оборудование, рационально использовать существующие и вновь вводимые новые вычислительные ресурсы и ресурсы хранения, реализовать программную виртуализацию серверов, а также придать дополнительный, расширенный функционал существующим средствам обработки и хранения данных, что, в конечном итоге, создает предпосылки для оптимизации расходов на создание и поддержание информационной инфраструктуры в любой точке местности. Вместе с тем, необходимо признать, что пока не существует единого подхода в вопросах управления МДЦ и в вопросах анализа и обеспечения их надежности, лишь недавно начали появляться документы (стандарты), регламентирующие процессы проектирования и эксплуатации различных дата-центров [2]. Все это делает безусловно актуальной проблему выработки системного подхода в вопросах оценивания и обеспечения надежности МДЦ, а также задачу разработки моделей и методов повышения технической надежности элементов таких систем (аппаратных, программных, иных) и, в целом, систем такого класса.

Решение предложенной проблемы на основе новых моделей и методов, позволит унифицировать механизмы оценивания и обеспечения надежности МДЦ и упростить внесение изменений в его инфраструктуру, будет способствовать повышению технической готовности и отказоустойчивости МДЦ, а также тиражируемости и масштабируемости структурных решений, нацеленных на повышение надежности систем такого класса.

По-прежнему, важно получить ответ на вопрос – как в условиях постоянного роста цены ресурсов получать максимальную отдачу от эксплуатации МДЦ. При этом возникают сопутствующие задачи, которые необходимо решать при управлении мобильными дата-центрами: как добиться существенного увеличения основных показателей надежности; каким образом при минимизации затрат учесть возможный рост нагрузки, предусмотреть восстановление полной работоспособности МДЦ после сбоев и отказов. Решение этих основных и сопутствующих задач возможно в рамках и по результатам процесса оценивания надежности МДЦ.

При этом, как фундаментальный этап, важным является решение задачи создания достоверных и оперативных алгоритмов оценивания надеж-

ности, которые позволят максимально точно, в оговоренные сроки и полноценно оценить надежность МДЦ с учетом динамики изменения условий их применения, а также с учетом неопределенности исходных данных, необходимых для принятия решения по управлению надежностью МДЦ.

Таким образом, несмотря на то, что существуют общемировые подходы к классификации (категоризации) надежности (Tier I, II, III, IV) дата-центров, единой методики оценивания надежности МДЦ не существует, поэтому направление исследований, на котором предполагается сосредоточиться при создании методики, и достоверных и оперативных частных алгоритмов многокритериального оценивания надежности МДЦ, нам видится состоящим из нескольких последовательных этапов:

Первый этап: формулировка системы показателей надежности МДЦ, а также синтез вероятностно-временной модели процесса смены состояний мобильного дата-центра, которая будет учитывать неопределенный характер изменения значений показателей надежности на основе методов применения математического аппарата условных вероятностей и методов гранулированных (гранулярных) вычислений [7].

Второй этап: разработка обобщенного и частных алгоритмов оценивания надежности МДЦ в условиях неопределенности.

Описание программных средств формирования и расчета надежности МДЦ в условиях неопределенности, а также рекомендации по использованию программно-алгоритмических средств при управлении надежностью и отказоустойчивостью МДЦ, могут составлять содержание третьего этапа.

И наконец, в рамках четвертого этапа возможно проведение проверки конструктивности разработанной методики и алгоритмов оценивания надежности МДЦ в условиях неопределенности. Проверка конструктивности позволит разработать научно-технические предложения по совершенствованию системы обеспечения надежности сложных мобильных информационных объектов такого класса.

Таким образом, рассмотрен новый подход к совершенствованию методологии и инструментария оценивания надежности современных мобильных дата-центров. Сформулированы частные задачи и проведено детальное описание этапов разработки методики многокритериального оценивания надежности мобильных дата-центров в различных условиях обстановки, с учетом различных аспектов неопределенности исходных данных, которые могут быть учтены в рамках математики гранулированных (гранулярных) вычислений. Планируется получить выигрыш в достоверности и оперативности оценивания надежности, что призвано способствовать повышению эффективности процесса информационной поддержки принятия решений по обеспечению надежности и отказоустойчивости мобильных дата-центров в условиях различного вида воздействий.

Список используемых источников

1. Концепция развития информационных и телекоммуникационных технологий Вооруженных Сил Российской Федерации на период до 2025 года (проект). М.: МО РФ, 2015. 16 с.

2. Национальный стандарт Российской Федерации ГОСТ Р 58811 – 2020. Центры обработки данных. Инженерная инфраструктура. Стадии создания. М.: Стандартинформ, 2020. 17 с.

3. Мобильный модульный центр обработки данных // ПитерЭнергоМаш. URL: http://piterenergomash.ru/index.php/katalog-produktsii/kontejnernye-resheniya/kontejnernye-tsod (дата обращения 19.12.2020).

4. Паращук И. Б., Михайличенко Н. В. Особенности построения и анализа качества дата-центров как базовых элементов IT-инфраструктуры // Перспективные направления развития отечественных информационных технологий: материалы IV Межрегиональной научно-практической конференции. Севастополь: Севастопольский государственный университет, 2018. 352 с., С. 28–29.

5. Google Unveils Its Container Data Center. Data Center Knowledge // Google (Alphabet). URL: https://www.datacenterknowledge.com/archives/2009/04 /01/google-unveils-its-container-data-center/ (дата обращения 20.12.2020).

6. Мобильные центры обработки данных // Инженерно-техническая компания «ИЛТОР». URL: https://iltor.ru/projects/data-centry/ (дата обращения 20.12.2020).

7. Бутакова М. А., Климанская Е. В., Чернов А. В. Формальные структуры и представления для гранулярных вычислений // Современные наукоемкие технологии. 2018. №5. С. 36–40.

УДК 004.657
ГРНТИ 50.41.21

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ ЭЛЕКТРОННОЙ ПРОДУКЦИИ

Г. А. Михаль, В. А. Тарасов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На сегодняшний день из-за большой конкуренции предприятия, производящие электронное оборудование, вынуждены находить новые способы оптимальной организации работы. Данный бизнес, как и любой другой, нацелен на прибыльную работу и выполнение всех требований заказчика в выделенные сроки. Многие процессы при проектировании печатных плат нуждаются в автоматизации. Крупные предприятия имеют средства на дорогостоящее программное обеспечение, а также в их штате, как правило, имеются программисты и системные администраторы, которые имеют соответствующие компетенции по работе с таким программным обеспечением, но у небольших

организаций на это нет средств. Бумажный документооборот, порождающий множество ошибок, нецентрализованное хранение файлов, библиотек, документации, приводят к большим задержкам в производстве, которые могут привести к колоссальным убыткам. Применяя новые технологии, предприятие систематизирует и автоматизирует работу, экономя тем самым трудовые и материальные ресурсы.

информационная система, электронная продукция, жизненный цикл, электронные компоненты, диаграмма прецедентов.

Для решения задачи проектирования информационной системы необходимо выделить основные сущности предметной области, описать связи между сущностями, определить акторов, взаимодействующих с системой, построить диаграмму вариантов использования.

Предметной областью базы данных, затронутой в данной статье, является информационная система управления жизненным циклом электронной продукции.

В связи с тем, что каждый компонент имеет общие атрибуты для всех категорий компонентов и специальные атрибуты для каждой категории, принято решение выделить набор общих для всех категорий атрибутов в отдельную сущность [1, 2, 3, 4].

Общие атрибуты характеризуются уникальным идентификатором компонента, обозначением, категорией, наличием компонента на торговых площадках. Каждый компонент в своей категории считается уникальным.

Изначально в системе неизвестно, какие категории компонентов будут использоваться в разработке электронной продукции. Предприятие, использующее систему, само будет добавлять данные сущности и выбирать их атрибуты с помощью предоставляемого программного обеспечения. Для данного функционала выделены список категорий и список специальных атрибутов для каждой категории как отдельные сущности.

Категории характеризуются уникальным идентификатором категории, названием категории, использующимся в системе, названием категории, использующимся для представления конечному пользователю системы. Название категории, использующееся в системе, является названием категории, использующимся для представления конечному пользователю системы с удалёнными пробелами и переведёнными в нижний регистр символами.

Список специфичных атрибутов характеризуется уникальным идентификатором специфичного атрибута, названием атрибута, использующимся в системе, названием атрибута, использующимся для представления конечному пользователю системы, описанием атрибута, категорией, контейнером атрибутов. Название атрибута, использующееся в системе, является назва-

нием атрибута, использующимся для представления конечному пользователю системы с удалёнными пробелами и переведёнными в нижний регистр символами.

Изначально в системе неизвестно, какие общие атрибуты компонентов будут использоваться в разработке электронной продукции. Предприятие, использующее систему, само будет добавлять общие атрибуты компонентов с помощью предоставляемого программного обеспечения. Для данного функционала выделен список общих атрибутов для компонентов как отдельных сущностей.

Список общих атрибутов характеризуется уникальным идентификатором общего атрибута, названием атрибута, использующимся в системе, названием атрибута, использующимся для представления конечному пользователю системы, описанием атрибута, контейнером атрибутов. Название атрибута, использующееся в системе, является названием атрибута, использующимся для представления конечному пользователю системы с удалёнными пробелами и переведёнными в нижний регистр символами.

Значения некоторых атрибутов могут браться из специальных контейнеров, которые предназначены для хранения часто повторяющихся значений атрибутов. Список данных специальных контейнеров выделен как отдельная сущность.

Контейнеры атрибутов характеризуются уникальным идентификатором контейнера атрибутов, названием контейнера атрибутов, использующимся в системе, названием контейнера атрибутов, использующимся для представления конечному пользователю системы, типом. Название контейнера атрибутов, использующееся в системе, является названием контейнера атрибутов, использующимся для представления конечному пользователю системы с удалёнными пробелами и переведёнными в нижний регистр символами.

Контейнеры атрибутов разделяются на типы в соответствии с тем, какие данные они в себе хранят. Список типов контейнеров атрибутов выделен в отдельную сущность.

Типы контейнеров атрибутов характеризуются уникальным идентификатором типа контейнера атрибутов, названием типа контейнера атрибутов.

Для структурирования компонентов на различные подразделы введена система каталогов как отдельная сущность.

Каталоги компонентов характеризуются уникальным идентификатором каталога компонентов, названием каталога компонентов, родительским каталогом.

Система привилегий пользователей выделена как отдельная сущность.

Пользователи характеризуются уникальным идентификатором пользователя, идентификатором учётной записи пользователя, паролем учётной

записи пользователя, привилегией добавления новых компонентов, привилегией изменения компонентов, привилегией удаления компонентов, привилегией просмотра логов, привилегией редактирования структуры библиотеки, привилегией редактирования структуры системы привилегий, привилегией редактирования «views».

Логирование посещения пользователями системы выделено как отдельная сущность.

Логи сессии характеризуются уникальным идентификатором, временем входа пользователя в систему, пользователем, вошедшим в систему.

Логирование изменений в библиотеке выделено как отдельная сущность.

Логи характеризуются уникальным идентификатором логов, временем, в которое произошло изменение, пользователем, совершившим изменение, названием компонента, с которым связано изменение, категорией компонента, с которым связано изменение, типом запроса на изменение, описанием деталей изменения.

Запросы на изменения в библиотеке разделяются на типы. Список типов запросов на изменения в библиотеке выделен в отдельную сущность.

Типы запросов на изменения в библиотеке характеризуются уникальным идентификатором типа запроса на изменения в библиотеке, названием типа запроса на изменение.

Выделены следующие связи между сущностями.

«Общие атрибуты – Список категорий» (M - 1) – каждый компонент относится к одной определённой категории, но одна категория может включать в себя множество компонентов.

«Общие атрибуты – Каталоги компонентов» (M - M) – каждый компонент может находиться в различных каталогах и один каталог может включать в себя множество компонентов.

«Каталоги компонентов – Каталоги компонентов» (M - 1) – каждый каталог может находиться только в одном каталоге, но один каталог может включать в себя множество каталогов.

«Список общих атрибутов – Контейнеры атрибутов» (M - 1) – каждый атрибут может брать значения только из одного контейнера, но один контейнер может предоставлять значения разным атрибутам.

«Список специфичных атрибутов – Контейнеры атрибутов» (M - 1) – каждый специфичный атрибут может брать значения только из одного контейнера, но один контейнер может предоставлять значения разным атрибутам.

«Список специфичных атрибутов – Список категорий» (M - 1) – каждый специфичный атрибут относится к одной определённой категории, но одна категория может включать в себя множество специфичных атрибутов.

«Логи – Список категорий» (M - 1) – каждая запись в логах относится к одной определённой категории, но одна категория может быть отмечена в нескольких записях.

«Логи – Типы запросов» (M - 1) – каждая запись в логах относится к одному типу запросов, но один тип запросов может быть отмечен в нескольких записях.

«Логи – Пользователи» (M - 1) – каждая запись в логах связана с одним пользователем, но один пользователь может быть связан с несколькими записями.

«Логи сессии – Пользователи» (M - 1) – каждая запись в логах сессии связана с одним пользователем, но один пользователь может быть связан с несколькими записями.

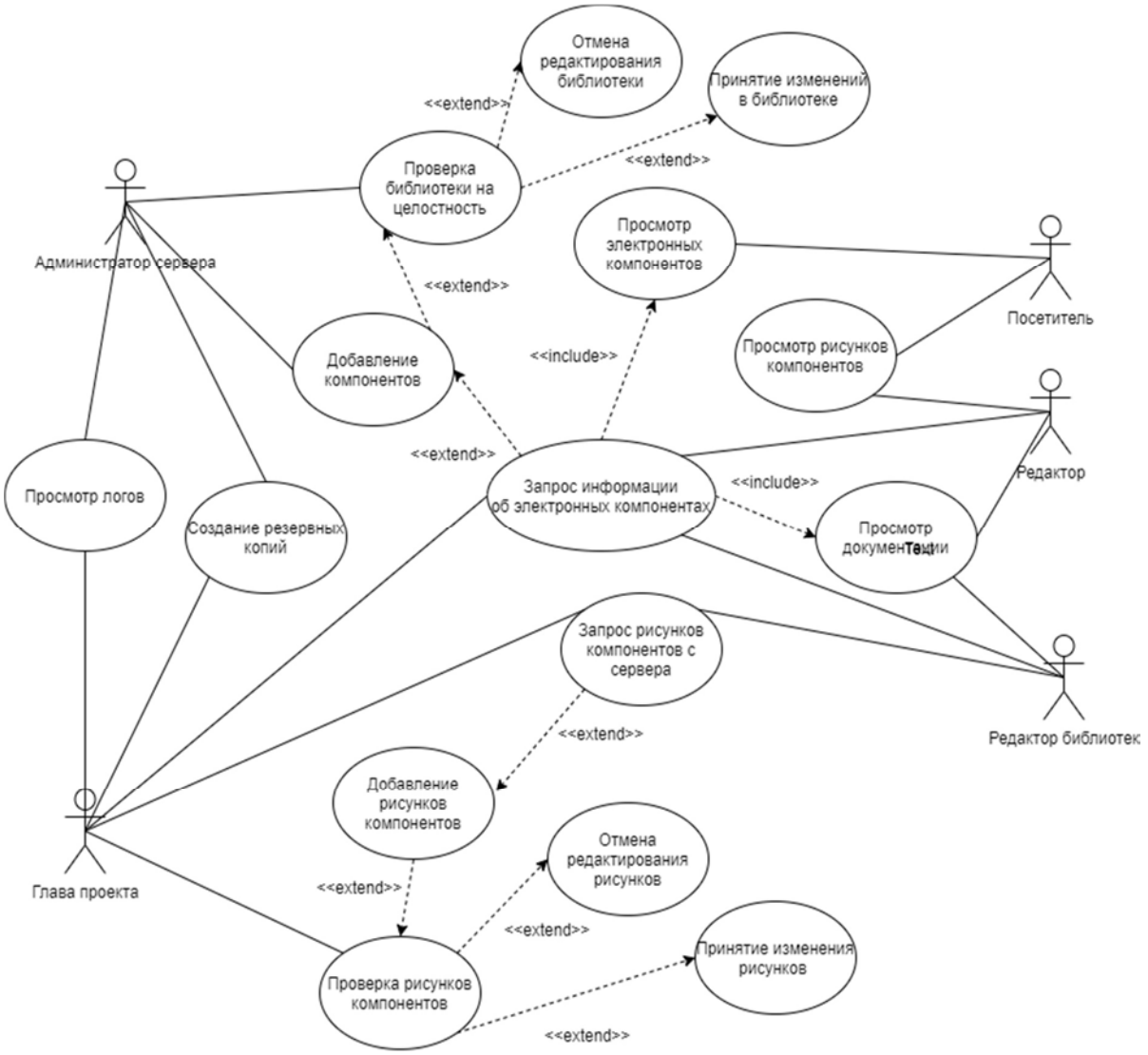


Рис. Диаграмма прецедентов

«Контейнеры атрибутов – Типы контейнеров атрибутов» (М - 1) – каждый контейнер атрибутов имеет один определённый тип, но один тип может относиться к нескольким контейнерам.

Выше проведён первичный анализ и выделены основные внешние и внутренние сущности предметной области. Материал, полученный в ходе работы, можно использовать в разработке информационных систем управления жизненным циклом электронной продукции.

При первичном анализе выделены следующие акторы: глава проекта, редактор библиотек, редактор, посетитель, администратор сервера. Акторы по отношению к проектируемой системе являются внешними сущностями. Как было отмечено выше, данные сущности взаимодействуют с системой и используют её функциональные возможности для достижения конкретных целей и решения частных задач.

Когда акторы выделены, можно приступать к построению диаграммы вариантов использования. Результат представлен на рис.

Список используемых источников

1. Руководство по MySQL. URL: https://metanit.com/ sql/mysql/ (дата обращения 13.01.2021).

2. Буч Г., Рамбо Д., Якобсон И. Язык UML. Руководство пользователя : пер. с англ. 2-е изд. М. : ДМК Пресс, 2006. 496 с.

3. Соловьев С. В., Гринкруг Л. С., Цой Р. И. Технология разработки прикладного программного обеспечения : учеб. пособие. М.: Акад. естествознания, 2011. 407 с. ISBN 978-5-91327-158-7.

4. Теория и практика UML. Диаграмма деятельности. URL: http://it-gost.ru/articles/view_articles/96 (дата обращения 24.05.2020).

Статья представлена заведующим кафедрой ИУС СПбГУТ, доктором технических наук, профессором Л. К. Птицыной.

УДК 004.891.2
ГРНТИ 06.35.51

КОНВЕРГЕНЦИЯ ТЕХНОЛОГИЙ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

Л. М. Монгуш, Г. Н. Смородин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Проведен анализ региональных технологических трендов цифровой экономики РФ. Показана возможность использования для описания динамики цифровой экономики концепции клубов конвергенции, используемой для анализа традиционных отраслей экономики и предложена соответствующая методика. На примере республик Сибирского федерального округа показана динамика разделения субъектов по клубам конвергенции.

цифровая экономика, технологические индикаторы, клубы конвергенции, конвергенция цифровых технологий.

Цифровая экономика (ЦЭ) занимает все более заметное место как в инновационных, так и традиционных компонентах экономического базиса страны [1].

Для оценки уровня развития ЦЭ принято использовать технологических подход – определять уровень развития ЦЭ на основе исследования тенденции роста технологических идентификаторов [2].

Анализ технологических индикаторов развития цифровой экономики

Проведенный анализ технологических индикаторов ЦЭ позволил выявить [3, 4]:

– отсутствие стандартного перечня технологий, отражающих развитие цифровой экономики;

– использование для оценки уровня развития ЦЭ, среди прочих, индикаторов технологий, не оказывающих существенного влияния на ЦЭ,

– использование индикаторов технологий, находящихся в течении нескольких лет в стадии насыщения, что воспринимается как цифровой шум и не позволяет выявить тренды развития ЦЭ,

– отсутствие статистической информации по технологиям, которые только начинают свой жизненный цикл и носят инновационный характер.

Также при исследовании было выявлено, что для оценки роста цифровой экономики целесообразно использовать понятие конвергенции, которое активно используется при анализе классической экономики [2].

Ряд регионов, имеющих индикаторы, близкие по значению и трендам развития, образуют один кластер развития или клуб конвергенции [2].

Сравнение развития регионов, не по отдельным индикаторам, а по региональным кластерам – региональным клубам конвергенции позволяет выявить параметры инновационного развития, возможно, свойственные только регионам данного клуба конвергенции.

По результатам анализа можно сформировать следующие выводы:

– технологические индикаторы позволяют формализовать оценку уровня развития цифровой экономики,

– близкие по значению и тренду индикаторы ЦЭ образуют кластеры, которые принято называть клубами конвергенции,

– исследование динамики клубов конвергенции предположительно позволит получить новые формализации по сравнению с исследованием отдельных индикаторов либо их совокупностей, сформированных без учета явления конвергенции.

Методика оценки уровня конвергенции технологий

С целью проверки положительного эффекта от применения концепции клубов конвергенции к оценке уровня развития ЦЭ предложена методика оценки конвергенции технологий, позволяющая формировать выборки из доступных массивов данных на основе заданных критериев.

Методика включает в себя процедуры:

– нахождения данных,

– очистки и структуризации данных,

– формирования массивов технологических индикаторов по виду технологий и временным параметрам,

– выбор индикаторов, обладающих характерной динамикой роста или падения,

– проведение сравнительного анализа индикаторов различных регионов,

– формализацию критериев принадлежности региона к клубам конвергенции,

– предварительную обработку данных (поиск и структуризацию),

– последующую формализацию результатов в виде динамики развития региональных клубов конвергенции.

Предлагаемая методика дает возможность:

– прослеживать динамику развития выбранных регионов, как членов клуба конвергенции по выбранному технологическому индикатору либо их совокупности,

– определять совокупность ключевых технологий, определяющих развитие или деградацию выбранного клуба конвергенций,

– прогнозировать переход регионов из одного клуба конвергенций в другой в результате изменения динамики развития индикаторов региона по сравнению с динамикой развития клуба конвергенции,

– при наличии показаний переходить от исследования развития регионов к исследованию развития клубов конвергенций.

Результаты применения методики

Для апробации методики были выбраны Сибирский федеральный округ, обладающей значительным разбросом значений цифровых индикаторов, что позволяет уменьшать уровень цифрового шума и более отчетливо показывать тренды развития локальных клубов конвергенции.

В качестве примера приведем динамику цифрового развития трех республик Алтай, Тыва и Хакасия. Индикатором цифровой экономики была выбрана технология широкополосного доступа в интернет.

Анализ показал наличие двух клубов конвергенции (рис.).

Рис. Динамика технологического индикатора

Первый клуб состоит из двух субъектов – лидеров по развитию анализируемой технологии и, предположительно, лидера по развитию цифровой экономики. Развитие технологии в данном клубе идет конвергентно.

Второй клуб представлен республикой Хакасия.

Между клубами наблюдается возрастающая дивергенция развития по выбранной технологии.

Выводы

На основании проведенных исследований можно утверждать, что:

– клубы цифровой технологической конвергенции являются эффективным инструментом определения тенденций развития ЦЭ,

– предлагаемая методика оценки уровня конвергенции технологий дает возможность ранжировать регионы как по уровню технологического развития, та и по его динамике,

– данная методика предусматривает дальнейшее развитие концепции клубов конвергенции с целью повышения достоверности результатов анализа технологического развития ЦЭ.

Продолжение исследований по теме конвергенции технологий предполагает разработку алгоритма автоматической селекции субъектов по клубам конвергенции, с возможным переходом субъекта из одного клуба в другой в случае изменения тренда развития технологии у данного субъекта по отношению к клубному тренду. Это позволит графически представлять не динамику развития отдельных субъектов, а динамику развития клубов.

Также представляется целесообразным разработать алгоритм определения технологий, наиболее адекватно отражающих развитие цифровой экономики в различных регионах. Предположительно, разным регионам будут соответствовать разные технологические индикаторы, определяющие их цифровое различие.

Список используемых источников

1. Минаков А. В., Евраев Л. О. Потенциал и перспективы развития цифровой экономики регионов России // Региональная экономика и управление. Электронный научный журнал. 2020. № 3 (63). URL: https://eee-region.ru/article/6318 (дата обращения 13.02.2021).

2. Блануца В. И. Перспективные экономические специализации для российских регионов в стратегии пространственного развития: клубы конвергенции // Экономика. Информатика. 2020. Т. 47, № 2. БГНИУ, Белгород. doi: 10.18413/2687-0932-2020-47-2-233-243.

3. Статистический ежегодник Республики Тыва, 2020: Стат.сб. / Красноярскстат. К78 Кызыл, 2020. 444 с.

4. Хакасский республиканский статистический ежегодник, 2020: Стат. сб. / Красноярскстат. К78 Абакан, 2020. 444 с.

5. Блануца В. И. 2018б. Социально-экономическое районирование в эпоху больших данных. М.: ИНФРА-М, 194 с.

УДК 004.94
ГРНТИ 20.01.07

ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ ВЕБ-ИНТЕРФЕЙСА ДЛЯ СЛАБОВИДЯЩИХ ПОЛЬЗОВАТЕЛЕЙ

Т. В. Мусаева, Ю. О. Украинец

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В жизни каждого человека довольно значимую роль играют цифровые технологии, скорость развития которых с каждым годом становится все больше и больше. Люди охотно пользуются теми возможностями, которые предоставляет им IT-сектор. Благодаря инновационным технологиям IT-сферы, человек легко может решать не только рабочие, но и повседневные задачи, но возникает вопрос: а все ли могут в одинаковой степени пользоваться возможностями, которые предоставляет нам данный рынок? К сожалению, не все пользователи взаимодействуют с цифровыми продуктами одинаково и очень часто, разрабатывая его, мы забываем о людях, возможности которых могут быть ограничены. Таким образом, на основе статистики и углубленно изученных современных методы проектирования пользовательского интерфейса для лиц, имеющих ограничения по зрению, в докладе будет представлен анализ, систематизация полученных данных и варианты решения актуальной на сегодняшний день проблемы.

дизайн система, ограниченные возможности, web технологии, ассистивные технологии, доступность.

Невозможно считать, что все пользователи взаимодействуют с цифровыми продуктами одинаково. Доступность становится решающим элементом дизайн-процесса. Не редко, разрабатывая IT-продукт, мы забываем о пользователях, возможности которых могут быть ограничены. Плохое зрение, слух, нарушение двигательных функций – лишь малая часть из всех тех особенностей, которыми может обладать человек.

Изучив статистику, обнаружено, что 56,7 млн американцев, 18,7 % населения страны, живут с одной из форм инвалидности. 38,3 миллиона американцев (12,6 % населения) имеют тяжёлую степень инвалидности. Это данные 2012 года, только для одной страны. Если подняться до мирового масштаба, показатели достигнут тревожных значений, и это уже не будет проблемой «меньшинства пользовательской базы». По данным федеральной службы государственной статистики, на 2020 год в России насчитывается 11 875 тысяч людей с инвалидностью (табл.) [1]. Полученные в ходе анализа результаты говорят о том, что проблема несет в себе глобальный характер и актуальна по сей день.

ТАБЛИЦА. Данные по количеству людей с инвалидностью на 2020 год

	2013	2014	2015	2016	2017	2018	2019	2020
Всего инвалидов, тыс. человек	13 082	12 946	12 924	12 751	12 261	12 111	11 947	11 875
в том числе: I группы	1 496	1 451	1 355	1 283	1 309	1 466	1 433	1 422
II группы	6 833	6 595	6 472	6 250	5 921	5 552	5 356	5 209
III группы	4 185	4 320	4 492	4 601	4 395	4 442	4 488	4 556
дети-инвалиды	568	580	605	617	636	651	670	688
Общая численность инвалидов, на 1 000 человек населения	91,3	90,1	88,4	87,0	83,5	82,5	81,4	80,9

Информация, поступающая извне, становится жизненно необходимым ресурсом, а как известно люди получают информацию благодаря органов чувств, преимущественно, с помощью глаз [2]. По данным ВОЗ 2019 года в мире насчитывается не менее 2,2 миллиарда случаев нарушения зрения или слепоты. Условно, людей, имеющих подобные проблемы можно разделить на три группы: плохо видящие, слабо видящие и невидящие. То, что проблемы со зрением или его полное отсутствие сильно ограничивают человека в решении различных задач, является неоспоримым фактом.

Психология дизайна – это сочетание нейробиологии, когнитивной психологии, социальной психологии и взаимодействия человека с компьютером. На основе данных, полученных в ходе исследований этих областей, создается дизайн пользовательского опыта. Так как люди со слабым зрением вынуждены опираться в основном на память и логику при взаимодействии устройствами для выхода в интернет, очень важно снизить их когнитивную нагрузку. В процессе анализа, был сделан вывод о том, что и зрячим и незрячим пользователям важна структура того или иного веб-ресурса (сайта, приложения и т. д.). Удобнее всего, когда текст на сайте структурирован по уровням заголовков, абзацам и тому подобному (рис. 1). Заголовки должны иметь минимально возможную длину, чтобы их можно было быстро прослушать и понять, есть ли на странице нужная человеку информация.

Человеку со зрительными нарушениями часто нужны вспомогательные средства для взаимодействия с веб-интерфейсом. Одним из примеров может служить доступность управления с клавиатуры [3, 6]. Соблюдая правила построения иерархии контента, можно сильно облегчить жизнь слабовидящим людям и снизить их когнитивную нагрузку при взаимодействии с веб-ресурсами [4]. Для корректного и комфортного взаимодействия с сайтами и (или) приложениями разработчику важно использовать правильную семантику

построения верстки сайта. При верстке элементов, имеющих особое назначение, таких как: списки, таблицы, заголовки и т. п. следует использовать строго определенные HTML-теги, что становиться намного проще, если на этапе дизайн-проектирования контент на сайте был соответствовал правилам построения визуальной иерархии [5]. Качественная верстка позволяет интегрировать сайты и приложения с ассистивными технологиями намного легче, что упрощает процесс взаимодействия.

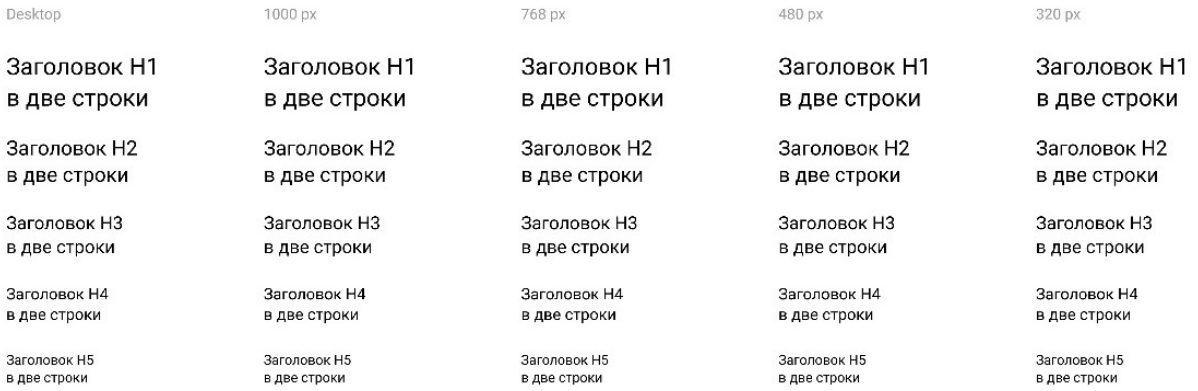


Рис. 1. Иерархичная структура заголовков

Для людей со зрительными нарушениями особенно важно, чтобы основной текст на сайте можно было легко прочитать с экранов разной яркости и качества. В соответствии с руководством по обеспечению доступности веб-контента (WCAG 2.0), текст на странице сайта и текст на изображениях должны иметь коэффициент контрастности не менее 4,5:1 (в рамках минимальных требований), что обязательно нужно учитывать, разрабатывая продукт, доступный каждому пользователю. Для создания оптимальной цветовой палитры, пример которой представлен на рис. 2, можно воспользоваться полезными сервисами: WEBAIM и Adobe Color.

Рис. 2. Пример оптимальной цветовой

WEBAIM включает в себя инструмент contrast checker, отображающий численное значение цветового контраста между двумя выбранными цветами, а генератором цветовых палитр Adobe Color, который благодаря наличию симулятора дальтонизма и функции, предупреждающей пользователя о конфликтных цветах, также является эффективным вспомогательным инструментом (рис. 3).

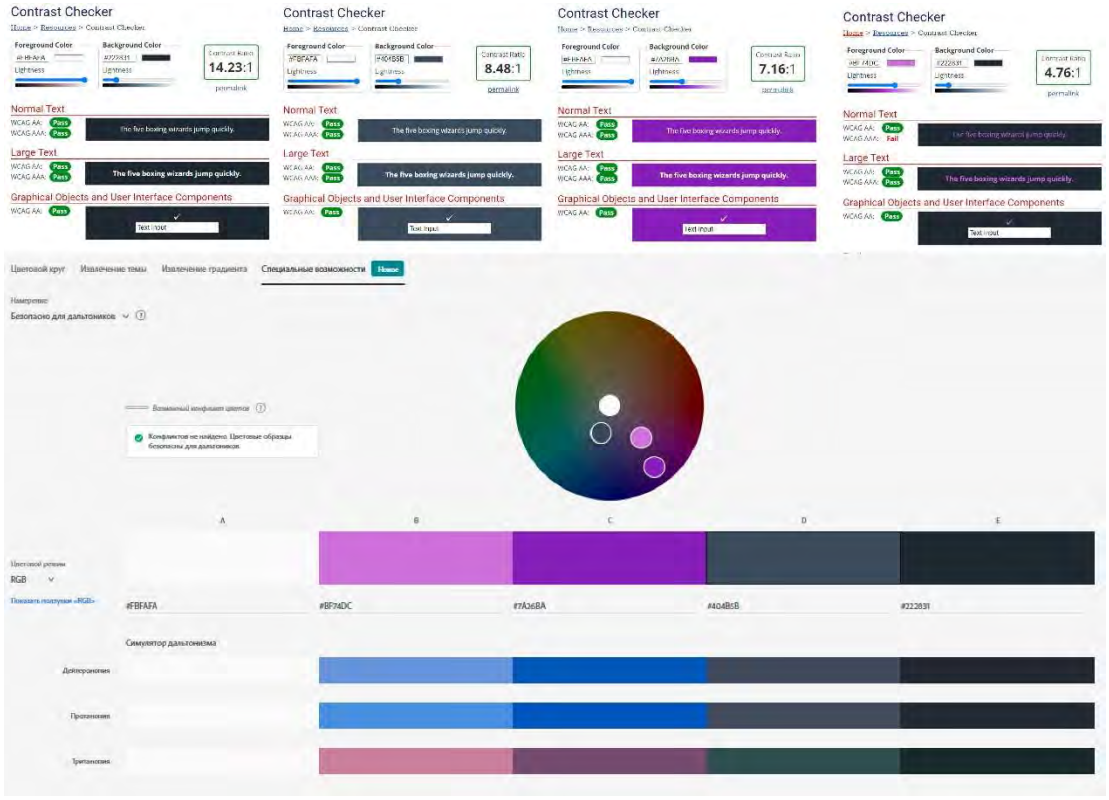


Рис. 3. Демонстрация результатов анализа составленной цветовой палитры с помощью метрик WEBAIM и Adobe Color соответственно

Увеличивая доступность продукта, мы улучшаем не только общее качество жизни людей современного мира, но и повышаем конверсию разрабатываемого продукта. Достижение 100 % доступности означает возможность использования полного функционала продукта абсолютно любыми пользователями (в том числе с ограниченными возможностями).

Список используемых источников

1. Харламова И. В., Овод С. В., Воронцова Е. А. Положение инвалидов. Уровень инвалидизации в Российской Федерации. Общая численность инвалидов по группам инвалидности // URL: https://rosstat.gov.ru/folder/13964?print=1

2. Тоффлер, Элвин. Третья волна. М. : АСТ, 2004. 781 с.

3. Web Accessibility Initiative (WAI). Web Content Accessibility Guidelines (WCAG) 2.0.

4. Как проверить визуальную иерархию? URL: https://tilda.education/articles-visual-hierarchy#rec16744185

5. Верстка сайтов для слабовидящих и людей с ограниченными возможностями/ URL: https://slabovid.ru/info/layout/

6. ГОСТ Р 52872-2019. Интернет-ресурсы и другая информация, представленная в электронно-цифровой форме. Приложения для стационарных и мобильных устройств, иные пользовательские интерфейсы. Требования доступности для людей с инвалидностью и других лиц с ограничениями жизнедеятельности

УДК 004.413
ГРНТИ 81.14.03

ОСОБЕННОСТИ УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С МЕТАУПРАВЛЕНИЕМ ФУНКЦИОНАЛЬНОСТЬЮ

А. А. Олимпиев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье описаны актуальные проблемы создания и сопровождения сложных программных систем, вызванные интенсивной динамикой развития информационных технологий. Рассмотрены особенности программных изделий, построенных с использованием различных способов организации взаимодействия заказчик-исполнитель. Определены возможные пути решения выявленной совокупности проблем, связанных с организацией управления жизненным циклом программных изделий, входящих в состав сложных автоматизированных систем.

управление проектами, жизненный цикл программного изделия, способы построения сложных программных систем.

Любая команда разработчиков специального программного обеспечения (СПО) рано или поздно сталкивается с широко известной проблемой создания адаптируемого повторно используемого решения. Данная проблема заключается в следующем: необходимо разработать такой комплект программ, который мог быть использован для автоматизации любой сферы человеческой деятельности, при этом стоимость и время адаптации к изменениям условий применения (программно-аппаратным платформам, новым потребностям пользователя, предметным областям и т.п.), а также затраты на сопровождение этого комплекта программ, должны быть минимальными.

Такой комплект программ представляет интерес и для потребителя при условии, что время и стоимость адаптации, а также базовая стоимость комплекта программ и стоимость его сопровождения будут меньше, чем у аналогов.

Для группы разработчиков данная проблема возникает, как правило, в момент, когда накоплено достаточно большое количество программного кода, который может быть повторно использован в новых проектах. Очевидным решением может служить оформление всего накопленного кода в виде совокупности программных библиотек, но такой подход экономически не достаточно эффективен, так как он позволяет лишь уменьшить объем

вновь разрабатываемого кода – то есть данный подход решает рассматриваемую проблему лишь частично. При этом данный подход, как правило, привносит достаточно большую избыточность в конечное изделие, стоимость которого в итоге неоправданно возрастает.

Современные исследования в области информационных технологий в этом направлении достигли определенных успехов (см. например, [3, 5, 6]), и для решения поставленной проблемы на сегодняшний момент ведущими специалистами предлагается целый ряд способов создания адаптируемого СПО.

Первый способ, наиболее распространенный среди программистов и архитекторов программного обеспечения, заключается в применении шаблонов проектирования, которые при грамотном использовании позволяют разработать СПО, адаптируемое за счет создания достаточно простых, небольших программных модулей, встраиваемых в программное изделие динамически или статически, а также оперативно модифицировать изделие под новое применение. Способ позволяет разработчикам получить максимальную выгоду от своего изделия за счет существенного сокращения времени и стоимости адаптации. Недостатком этого способа является заложенное в конструкцию ограничение на наращивание прикладных задач. Преодоление такого ограничения в большинстве случаев возможно только за счет изменения конструкции СПО.

Второй способ, как правило, используется в WEB-приложениях, но может применяться и в других ситуация, и заключается в разработке так называемых «программ-конструкторов» приложений – адаптация СПО осуществляется аналогично с первым способом. Разница заключается в том, что готовая система полностью открыта и может изменяться силами пользователя, если он обладает достаточной квалификацией. В системах, построенных вторым способом определенным образом разрабатывается ядро системы, к которому может быть подключено любое приложение, то есть связь между ядром и приложением слабая, в отличие от первого способа. Недостатком данного способа является большой объем работы, который требуется выполнить для реализации нового приложения, если отсутствует соответствующая «заготовка». Вторым недостатком данного способа является низкая скорость работы приложения, что существенно ограничивает область применения этого способа.

Третий способ заключается в применении приемов методологии метауправления функциональностью – создании программной системы в виде комплекта интерпретаторов языков высокого и сверхвысокого уровней, для которых реализован программный интерфейс обмена данными [4]. Речь идет о создании «программ-конструкторов» сложных программных систем. Используемые интерпретаторы и языки могут быть практически любыми, поэтому такое решение может быть адаптировано под конкретную

группу разработчиков и пользователей с точки зрения их квалификации. Основной особенностью данного способа является наличие средства обмена сообщениями между интерпретаторами, которые могут находиться на разных ЭВМ — обмен данными происходит прозрачно для разработчика за счет расширения контекстной библиотеки используемых интерпретаторов. Недостатком способа является сложность реализации конкретного приложения, обеспечения целостности тех данных, которые одновременно обрабатываются разными модулями, и обеспечения совместимости между используемыми языками.

Четвертый способ заключается в реализации программного изделия в виде микроядра и расширения, которое периодически обновляется микроядром с выделенного ресурса. Обновления такого программного обеспечения могут регулярно выкладываются разработчиками. Данный способ является предельно простым с точки зрения реализации и позволяет добиться непрерывного развития программной системы и оперативного ее обновления за счет достаточно тесной интеграции среды разработки и пользовательских приложений. Недостатком данного способа является ограниченная возможность со стороны пользователя контролировать вносимые в СПО изменения и, следовательно, необходимость в высоком уровне доверия между заказчиком и исполнителем-монополистом.

Перечисленные способы достаточно похожи друг на друга с точки зрения реализации, их основное отличие заключается в стратегии получения прибыли. При создании СПО для сложных автоматизированных систем все эти способы должны применяться совместно, за счет чего может быть достигнута высокая эффективность с точки зрения экономии времени и денежных средств как потребителя, так и исполнителя. Следовательно, может быть достигнута высокая конкурентная способность конечного изделия на рынке.

Однако, при выборе из существующих оптимального или разработке нового комплексного решения руководителю проекта и главному конструктору предстоит решить ряд проблем, к которым в первую очередь относятся:

– проблема формирования системы управления жизненным циклом [2], в особенности, организации этапов производства, подготовки производства и сопровождения СПО как программного изделия;

– проблема разработки или выбора инструментальных средств, библиотек и проблемно-ориентированных языков [3, 6], которыми будут оснащены автоматизированные средства управления конфигурацией и версиями программного изделия и само изделие;

– проблема формирования, обучения и содержания команды разработчиков, обладающих достаточной квалификацией и являющихся носителями необходимых компетенций.

На сегодняшний день не существует готового решения и, тем более, стандарта, позволяющего в разумные сроки и за разумные деньги запустить промышленную технологию производства СПО, в которой были бы решены одновременно все вышеперечисленные проблемы.

Причиной сложившейся ситуации, с одной стороны, служит интенсивное развитие информационных технологий в области решения прикладных задач с помощью СПО, которое в атмосфере рыночной экономики порой принимает непредсказуемый характер. Это объясняется тем, что сегодняшняя ситуация во многом зависит от «моды» на популярные языки программирования, инструменты и библиотеки, которые «нравятся большинству» программистов, и приводит к тому, что многие прикладные программные решения «устаревают» (выходят из моды) раньше, чем успевают выйти на рынок, а компетенции не успевают полностью сформироваться, либо быстро становятся не нужными, в итоге от рядового специалиста требуется уровень значительно превышающий необходимый минимум.

С другой стороны, многие решения, касающиеся одной проблемы, влияют на другие аспекты. Так, например, от выбора инструментальных средств и языка описания функциональности могут зависеть компетенции рабочей группы, а также состав, последовательность, стоимость и длительность технологических операций, входящих в процесс производства и сопровождения СПО.

Третьим моментом, на который следует сделать акцент — это последствия влияния рыночной экономики на динамику кадров: на рынке труда наблюдается рост процента недобросовестных исполнителей, который происходит на фоне необъективного завышения ими стоимости выполнения отдельных технологических операций; наблюдается дефицит квалифицированных специалистов, которых становится все сложнее выявить.

Для ослабления напряжения, связанного с описанными проблемами, и повышения экономической эффективности деятельности предприятий-разработчиков СПО необходимо разрабатывать комплексные подходы, включающие в себя [1, 2]:

– оценку экономической эффективности принимаемых решений в текущей рыночной обстановке и меняющихся тенденций развития информационных технологий;

– применение передовых и разработку новых подходов к управлению компетенциями и проектами;

– совершенствование существующих и разработку новых методов и методик автоматизации управления жизненным циклом программного изделия;

– совершенствование существующих и разработку новых методов и методик управления рисками.

Список используемых источников

1. Боронина Л. Н. Основы управления проектами. М-во образования и науки Рос. Федерации, Урал. федер. ун-т. Екатеринбург: Изд-во Урал. ун-та. 2015. 112 с.
2. Косяков А., Свит У. и др. Системная инженерия. Принципы и практика. Пер. с англ. под ред. В. К. Батоврина. М.: ДМК Пресс, 2017. 624 с.
3. Ларман, Крэг. Применение UML 2.0 и шаблонов проектирования, 3-е изд. : Пер. с англ. М.: ООО «И.Д. Вильямс», 2018. - 736 с.
4. Олимпиев А. А. Методика синтеза системы оперативно-технического мониторинга с метауправлением функциональностью. Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2018. Т. 2. С. 505–510.
5. Фаулер М. Архитектура корпоративных программных приложений.: Пер. с англ. М.: Издательский дом «Вильямс», 2006. 544 с.
6. Эванс Э. Предметно-ориентированное проектирование структуризация сложных программных систем: пер. с англ. М.: ООО «И.Д. Вильямс», 2011. 488 с.

УДК 004.056.5
ГРНТИ 81.96

РАЗДЕЛЕНИЕ КЛЮЧА ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СИСТЕМЫ ТАЙНОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Д. А. Орлов, В. А. Яковлев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается система электронного голосования на основе гомоморфной криптографической системы Пэйе. Представлены предложения по разделению секрета (ключа расшифрования), определено рациональное количество долей и определены участники избирательного процесса, которым эти доли предоставляются до начала голосования. Предлагается процедура восстановления закрытого ключа участниками перед началом подсчета голосов.

система электронного голосования, разделение секрета, криптосистема Пэйе, схема разделения секрета Педерсена.

Электронное голосование – термин, определяющий различные виды голосования, охватывающий как электронные средства голосования, так и технические электронные средства подсчета голосов. Одной из разновидностей электронного голосования является процедура выборов посредством

сети Интернет. Данная технология, по сравнению с традиционным голосованием, позволяет с более высокой скоростью обрабатывать бюллетени, экономить время на их заполнение, отображать ход голосования в реальном времени, а также способна эффективно масштабироваться. При этом участникам выборов не требуется приходить на избирательный участок, что позволяет облегчить процедуру голосования.

В соответствии с [1] к основным участникам избирательного процесса относятся:

- избиратели;
- избирательные объединения;
- кандидаты;
- избирательные комиссии;
- члены избирательных комиссий с правом решающего и совещательного голоса;
- уполномоченные представители кандидатов и избирательных объединений;
- доверенные лица кандидатов и избирательных объединений;
- наблюдатели, международные (иностранные) наблюдатели;
- средства массовой информации и их представители;
- государственные органы, органы государственной власти и органы местного самоуправления и их должностные лица.

Рассмотрим систему электронного голосования в предположении, что обеспечение тайны голосования осуществляется на основе гомоморфной криптосистемы Пэйе [2]. Применение данной криптосистемы обеспечивает тайну голоса, поданного избирателем, для всех участников избирательного процесса, в том числе и для избирательной комиссии, повышает точность и оперативность подсчета голосов.

В этой криптосистеме генерируются ключи: открытый ключ pk и закрытый ключ sk. Открытые ключи избиратели получают после их идентификации в системе. Бюллетени, содержащие выбор избирателей (число), шифруются открытым ключом pk и отправляются на сервер. Сервер, приняв криптограммы от всех избирателей, перемножает их и отправляет полученное значение (криптограмму-произведение) в избирательную комиссию. Избирательная комиссия расшифровывает полученную криптограмму с помощью секретного ключа sk и определяет сумму голосов, поданных за каждого кандидата.

Достигается это за счет гомоморфного свойства криптосистемы Пэйе, заключающегося в следующем [2]: при расшифровании произведения нескольких шифротекстов будет получена сумма соответствующих им открытых текстов, то есть $D(E(m_1) * E(m_2)\ mod\ n^2) = (m_1 + m_2)\ mod\ n$, где E

и D – операции шифрования и расшифрования соответственно. Таким образом, подсчет зашифрованных голосов дает сумму всех голосов, что обеспечивает анонимность голоса каждого избирателя.

Однако описанная схема имеет ряд уязвимостей:

− уязвимость, при которой избирательная комиссия при сговоре с сервером может подделать голоса избирателей;

− уязвимость, при которой избирательная комиссия расшифровывает голоса раньше поставленного срока и оказывает влияние на дальнейший процесс голосования (агитация, «вброс голосов»).

Для защиты от таких атак необходимо разделить ключ расшифрования криптограммы на несколько долей, таким образом, чтобы доли ключа по отдельности были бесполезны. Решается такая задача применением схем разделения секрета.

Проанализированы следующие схемы разделения секрета:

− схема разделения секрета Шамира;

− схема разделения секрета Асмуса-Блума;

− схема проверяемого разделения секрета Фельдмана;

− схема проверяемого разделения секрета Педерсена.

Схема Шамира и схема Асмуса-Блума не позволяют проверить корректность долей секрета, поэтому участник разделения не может с полной уверенностью сказать, что его доля является подлинной. Также, данные схемы предполагают, что дилер, который генерирует и раздает доли, надежен, однако данное утверждение не всегда является истинным.

Схема Фельдмана и схема Педерсена относятся к классу схем проверяемого разделения секрета, которые предоставляют всем участникам разделения возможность проверить, что ими были получены корректные доли секрета. Такие схемы предназначены для случаев, когда участники разделения не могут доверять друг другу, в том числе и дилеру.

Схема Фельдмана [3] обладает теоретико-сложностной стойкостью и базируется на вычислительной сложности задачи дискретного логарифмирования, т.е. нахождения значений s_i при известном $z_i = g^{s_i}$.

В схеме Педерсена [4] помимо свойства гомоморфизма дискретного логарифма, используется схема обязательства, которая позволяет скрыть секрет, даже если вычислительно неограниченный противник умеет решать задачу дискретного логарифмирования, что обеспечивает теоретико-информационную стойкость протокола. Поэтому для дальнейшего анализа выбрана (k, n)-схема Педерсена, где n – общее число участников разделения секрета, k – минимальное число участников, необходимое для восстановления общего секрета $\left(k \geq \frac{n+1}{2}\right)$.

Для этой схемы определим следующие параметры:

− p, q – большие простые числа, $p - 1 \equiv 0\ (mod\ q)$;

− g – элемент порядка q группы Z_p^*, т. е. $g^q \equiv 1(mod\ p)$;

– $h \in Z_p^*$ – открытое общедоступное число, такое, что $d \in Z_q$, где $g^d = h\ (mod\ p)$, неизвестно никому, в том числе дилеру.

Чтобы распределить секрет s, дилер, которым в избирательной схеме является оператор системы, назначенный территориальной комиссией, выбирает два многочлена $Q(\cdot)$, $F(\cdot)$ степени $k-1$ над полем Z_q с коэффициентом $Q_0 = s$ и случайными коэффициентами $\{Q_m\}_{m\in\{1,\dots,k-1\}}$ и $\{F_m\}_{m\in\{0,\dots,k-1\}}$ соответственно, т. е.

$$Q(x) = Q_0 + Q_1 x + Q_2 x^2 + \cdots + Q_{k-1} x^{k-1} \in Z_q[x], \qquad Q_0 = s,$$

$F(x) = F_0 + F_1 x + F_2 x^2 + \cdots + F_{k-1} x^{k-1} \in Z_q[x]$, $F_0 -$ случайное число, и распространяет всем участникам P_i, $i = \overline{1,n}$, открытую величину $E_m = g^{Q_m} * h^{F_m}\ (mod\ p)$, $m = \overline{0,k-1}$. Затем дилер секретно пересылает всем участникам P_i, $i = \overline{1,n}$ их доли $\{s_i, t_i\}$, где $s_i = Q(i)$, $t_i = F(i)$.

Участник P_i может проверить корректность своей доли, проверив равенство

$$g^{s_i} h^{t_i} =^{?} (E_0) * (E_1)^i * (E_2)^{i^2} * \dots * (E_{k-1})^{i^{k-1}}\ (mod\ p).$$

При положительном результате проверки будет выполнено равенство

$$(g^{Q_0} h^{F_0}) * (g^{Q_1} h^{F_1})^i * \dots * (g^{Q_{k-1}} h^{F_{k-1}})^{i^{k-1}} =$$
$$= g^{Q_0 + Q_1 i + \cdots + Q_{k-1} i^{k-1}} * h^{F_0 + F_1 i + \cdots + F_{k-1} i^{k-1}} = g^{Q(i)} * h^{F(i)}\ (mod\ p).$$

Если k или более пользователей объединяют свои индивидуальные доли, то они смогут восстановить полином, используя интерполяционную формулу Лагранжа:

$$Q(x) = \sum_{S=1}^{k} s_{i_S} \prod_{\substack{j=1 \\ j\neq S}}^{k} \frac{(x - x_{i_j})}{(x_{i_S} - x_{i_j})}\ mod\ p.$$

Предлагается следующее разделение долей секрета среди участников избирательного процесса:

– председатель (или заместитель председателя) территориальной избирательной комиссии – 1 доля;

– председатель (или заместитель председателя) избирательной комиссии муниципальных образований – 2 доли;

– члены избирательных комиссий с правом решающего голоса – 3 доли, что соответствует минимально возможному количеству членов участковой комиссии с правом решающего голоса [5];

− члены избирательных комиссий с правом совещательного голоса – 1 доля;

− руководитель (или заместитель руководителя) общественного штаба – 1 доля;

− руководитель (или заместитель руководителя) корпуса наблюдателей – 1 доля.

Разделение ключа расшифрования sk производится участковой избирательной комиссией, закрепленной за местом проведения голосования, начинается после завершения генерации пары ключей голосования и осуществляется на специально выделенном компьютере.

Этапы:

− разделение ключа расшифрования с помощью схемы проверяемого разделения секрета Педерсена на специальном компьютере в присутствии хранителей. Предлагается использовать (5,9)-пороговую схему, в которой ключ разделяется на 9 долей, а восстановление ключа производится из 5 долей, при этом допускается не более $\frac{n-1}{2} = 4$ нечестных участников;

− запись долей секрета на защищенные съемные носители;

− проверка правильности долей (проводится дилером в присутствии участников разделения для предотвращения нарушений со стороны дилера);

− помещение съемных носителей в номерные сейф-пакеты и передача их хранителям;

− запечатывание компьютера в пакет с экранирующим слоем, упаковка в кейс и отправление на хранение в избирательную комиссию.

Восстановление ключа расшифрования производится участковой избирательной комиссией, закрепленной за местом проведения голосования, и начинается в назначенное время после завершения этапа подсчета голосов на компьютере, на котором проводилось формирование ключей и разделение ключа расшифрования.

Этапы:

− встреча хранителей долей секрета для восстановления ключа;

− распечатывание компьютера;

− считывание долей секрета со съемных носителей;

− проверка правильности долей (проводится дилером в присутствии участников разделения для избегания нарушений со стороны хранителей долей секрета);

− восстановление ключа расшифрования согласно схеме проверяемого разделения секрета Педерсена;

− загрузка ключа расшифрования в систему и начало процесса расшифровки голосов.

Поскольку для восстановления ключа достаточно 5 долей, то из этого количества и предлагается восстанавливать секрет. При этом доли, используемые для восстановления, могут определяться посредством случайного

выбора из числа лиц, успешно прошедших процедуру проверки. Также имеется возможность проведения проверки корректности конкретной доли по запросу, поскольку каждый участник имеет все необходимые для проведения проверки значения.

Если какая-либо доля окажется некондиционной после процесса разделения ключа расшифрования, то процесс генерации ключей и разделения ключа расшифрования начинается заново. Если же доля оказалась некондиционной до процесса восстановления ключа, то такая доля не участвует в процессе восстановления и «отбрасывается».

Список используемых источников

1. Участники избирательного процесса. URL: https://izbirkom.rkomi.ru/cdo/?id=386#a6 (дата обращения 09.03.2021).

2. Paillier, P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes // Advances in cryptology, EUROCRYPT'99, 1999. С. 223–238.

3. Feldman, P. A Practical Scheme for Non-interactive Verifiable Secret Sharing // IEEE Symposium on Foundations of Computer Science, 1987. Pp. 427–437.

4. Pedersen T. P. «Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing» // EUROCRYPT’91, 1991. Pp. 129–140.

5. Федеральный закон «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» от 12.06.2002 N 67-ФЗ.

УДК 654.024
ГРНТИ 49.39.29

ИССЛЕДОВАНИЕ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ СПЕЦИАЛЬНЫХ СИСТЕМ ТЕЛЕКОММУНИКАЦИЙ В УСЛОВИЯХ НЕОПРЕДЕЛЁННОСТИ

А. А. Павлович[1], **А. С. Присяжнюк**[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]ЗАО «Институт телекоммуникаций»

Рассматриваются известные результаты исследования специальных систем телекоммуникаций (ССТ) и влияние неопределённостей на математические методы оценивания их функциональной устойчивости, а также выбор варианта построения ССТ на основе эксперимента.

системы телекоммуникаций, моделирование, функциональная устойчивость, деструктивные воздействия, эффективность/

Анализ результатов полемики по проблеме обоснования технических путей обеспечения функциональной устойчивости (ФУ) специальных систем телекоммуникаций (ССТ) позволяет прогнозировать, что в перспективе эти мероприятия будут планироваться и решаться в качестве отдельной задачи. В последнем случае мероприятия по обеспечению ФУ ССТ целесообразно рассматривать как составную часть процесса планирования. При планировании ССТ особенностью является невозможность однозначно предсказать эффективность выполнения мероприятий по обеспечению её ФУ на основе имеющейся априорной информации. Процесс обеспечения ФУ ССТ подчиняется определенным объективным законам, однако, эти законы проявляются через множество неопределенностей.

Большинство «элементарных» процессов, составляющих процесс обеспечения ФУ ССТ, носят случайный характер (факты воздействия, последствий воздействий, восстановления ССТ за установленный период времени являются случайными событиями). При этом процессы подготовки принятия решений призваны снизить элемент случайности и придать этим процессам детерминированный целенаправленный характер, однако элемент случайности в процессе обеспечения ФУ ССТ в условиях внешних деструктивных воздействий всегда присутствует. Это служит основанием для применения стохастических моделей при исследовании данного процесса.

Решая стохастическую задачу целесообразно использовать методы теории вероятностей. Использование вероятностных методов позволяет, минуя слишком сложное исследование всех по отдельности случайных явлений, обратиться непосредственно к законам, управляющим массами таких явлений. Кроме того, использование вероятностных методов позволяет прогнозировать явления, ограничивать сферу деятельности случайности и сужать ее влияние на практику.

В процессе обеспечения ФУ ССТ в условиях внешних деструктивных воздействий опираются на методы, учитывающие стохастичность рассматриваемого процесса. Для решения однокритериальной статической стохастической задачи целесообразно использовать прием сведения стохастической задачи к детерминированной путем оптимизации в среднем. При этом для каждой стратегии по обеспечению ФУ ССТ, вычислить вероятности $P(t)$ возможных исходов решаемых задач и соответствующие показатели эффективности функционирования при этих исходах. Затем для каждого результата определить математическое ожидание показателя эффективности и выбрать ту стратегию по обеспечению ФУ ССТ, для которой эффективность имеет лучшее (экстремальное) значение.

Следует отметить, что ССТ характеризуются наличием достаточно большого информационного обмена между абонентами, в котором значи-

тельную роль играет элемент случайности. Кроме того, в процессе обеспечения ФУ ССТ приходится учитывать случайный характер поведения абонентов. Поэтому, при оценивании ФУ целесообразно использовать методы теории массового обслуживания. С учетом специфики выполнения требований, предъявляемых к ССТ, целесообразно использовать систему массового обслуживания (СМО). СМО необходимо описывать простейшими (пуассоновскими) потоками случайных событий. С учетом воздействий на ССТ деструктивных воздействий, необходимо использовать многоканальную (n-канальную СМО) с производительностью обработки информации – μ и общей производительностью – $n \cdot \mu$.

При моделировании ССТ в условиях внешних деструктивных воздействий необходимо использовать схемографические модели, в основе которых положено представление ССТ конечным ориентированным и кратных ребер графом – $G(N,M)$, в котором вершинам – N соответствуют множество элементов ССТ $n_1, n_{2,} \ldots . n_n$, а ребрам M – множество ветвей рассматриваемых систем $m_1, m_{2,} \ldots . m_n$.

При оценивании ФУ ССТ и обосновании технических путей её обеспечения в условиях внешних деструктивных воздействий необходимо использовать оптимизационные методы, которые позволяют на основе количественных оценок вариантов решений выбирать лучший, избегая полного перебора всех возможных вариантов.

Данный подход позволяет выбрать наиболее рациональный метод оптимизации процесса обеспечения ФУ ССТ с учетом уровня, при этом учитываются не только оценки показателей основных свойств ССТ, но и изменяющиеся условия функционирования источника деструктивных воздействий.

При исследовании ССТ в рассматриваемых условиях, необходимо учитывать случайную природу воздействий. Чтобы постоянно корректировать уровни управляемых факторов, отвечающие экстремуму, необходимо непрерывно вести его поиск для приспосабливания к изменившимся условиям, то есть проводить адаптационную оптимизацию. Адаптационная оптимизация предполагает оценивание коэффициентов регрессии при быстрых флуктуациях неконтролируемых факторов, которые влияют на эффективность функционирования ССТ, в результате чего ошибка значительно возрастает по сравнению со способами линейного и динамического программирования. Чтобы получить значимые оценки коэффициентов регрессии управляемых факторов при достаточно большой величине ошибки опыта, следует увеличить число параллельных опытов и шаги варьирования факторов. Непрерывный поиск экстремума при очень большом числе парал-

лельных опытов нецелесообразно осуществлять с помощью способов линейного и динамического программирования, так как это потребовало бы реализации чрезвычайно громоздкого экстремального эксперимента.

Адаптационная оптимизация процесса оценки ФУ ССТ позволяет одновременно с выполнением основной функции данного процесса получать полезную информацию для нахождения оптимальных условий деструктивных воздействий. Для этого необходимо изменять в разные стороны управляемые факторы с помощью пробных возмущений и выделять слабое влияние изучаемых базисных функций на фоне воздействий, накапливая результаты проведенных параллельных опытов. В основе адаптационной оптимизации лежит метод эволюционного планирования (ЭВОП) [2]. Его основными чертами являются небольшое варьирование управляемыми факторами и отбор вариантов, наилучших с точки зрения заданного критерия оптимизации. Изучение небольшой группы коэффициентов регрессии управляемых факторов представляет собой фазу проведения эксперимента:

$$y_i = \pm x_0 b_0 \pm x_1 b_1 \pm \ldots \pm x_i b_i . \quad (1)$$

После проведения одной фазы необходимо перейти к новой с исследованием новых условий, включая другие уровни тех же факторов или другие факторы. Каждая из фаз содержит последовательность m параллельных циклов. Цикл любой фазы состоит из нескольких опытов для различных вариантов варьирования уровней факторов данной фазы. Многократное повторение циклов, то есть проведение для каждого варианта варьирования m параллельных опытов, уменьшает ошибку среднего арифметического из результатов m наблюдений в $\sqrt{m}$. По окончании каждого цикла производится математическая обработка результатов наблюдений, а по завершении каждой фазы принимают решение, как планировать следующую фазу.

Предлагается порядок проведения эксперимента:

1. Составление таблицы равномерно распределенных случайных величин:

– выбор начальной точки x_0 (начальная фаза операции);

– отбор для каждой фазы n управляемых факторов;

– выбор величины пробных шагов варьирования Δx_i по каждому управляемому фактору x_i данной фазы;

– выбор в качестве программы цикла план типа 2^n или план типа 2^{n-1} с одной или двумя центральными точками (двумя – при разбиении факторного эксперимента на два ортогональных блока).

2. Проведение эксперимента. Математическая обработка результатов наблюдений происходит с помощью оценивания коэффициентов регрессии,

смещения среднего, ошибки воспроизводимости, точности выборочных коэффициентов регрессии и смещения среднего.

3. Осуществляется систематизация собранной информации и формулировка выводов.

Кроме того, при оценивании ФУ ССТ в условиях внешних деструктивных воздействий целесообразно использовать [1, 2]:

– теорему Реньи при определении оптимальной селекции сообщений, циркулирующих в системе;

– теорему единственности и мультипликативное свойство характеристической функции при определении эффективности информационного взаимодействия между элементами системы;

– модель Фишборна при определении показателя эффективности комплексного применения разнородных средств и ресурсов;

– градиентно-разностный метод при моделировании процесса планирования мероприятий по обеспечению ФУ ССТ.

Одной из основных задач, решаемых в рассматриваемом случае, является выбор варианта построения ССТ с учетом внешних деструктивных воздействий в момент времени t. Выбор рационального варианта определяется целенаправленностью рассматриваемых процессов.

Подход к формализации задачи выбора, не требующий построения обобщенного скалярного показателя эффективности, исходит из того, что формирование решений по выбору рационального варианта построения ССТ формально может быть представлено в виде [1, 2]:

$$(W, Q, A) \underset{\text{П}}{\rightarrow} W^*, \tag{2}$$

где $W = \{w_k, k = 1,2,...,K\}$ – множество возможных вариантов построения ССТ;

k – идентификатор;

K – количество вариантов построения ССТ;

$Q = \{Q_n(w_k), n = 1,2,...,N, k = 1,2,...,K\}$ – множество (вектор) показателей, по которым оценивается эффективность функционирования ССТ;

$Q_n(w_k), n = 1,2,...,N, k = 1,2,...,K$ – частный скалярный показатель эффективности функционирования ССТ;

$A = \{a_n, n = 1,2,...,N\}$ – множество коэффициентов важности частных скалярных показателей эффективности, причем $\sum_{n=1}^{N} a_n = 1$, где n и N – идентификатор и количество частных показателей;

$W^* = \{w_{k1} \succ w_{k2} \succ ... \succ w_{k\psi}\}$ – упорядоченное по эффективности подмножество предпочтительных вариантов построения ССТ;

ψ – количество предпочтительных вариантов;

$\succ$ – знак отношения доминирования;

$П$ – критерий оптимальности, то есть правило, определяющее как, используя показатель Q, выделить из множества W альтернативных вариантов подмножество W^* предпочтительных.

При такой формализации для выбора оптимального варианта построения ССТ возможно использовать известные в науке метод Парето, Черчмена-Акофа, Терстоуна, Неймана-Моргенштерна, мажоритарный метод, ранговый метод и др. [1, 2].

Таким образом, для решения выше сформулированной проблемы обоснования технических путей обеспечения функциональной устойчивости ССТ целесообразно использовать метод выбора с доминирующим показателем. Особенность метода состоит в том, что один из показателей эффективности ССТ (например, показатель ФУ ССТ – $Q_1(w_i), i = 1,...,K$) является главным, а остальные $Q_n(w_i), i = 1,...,K, n = 2,...,N$ дополнительными. Вариант w_i считается лучшим в том случае, если он имеет наибольшее значение главного показателя, либо превосходит по некоторым дополнительным показателям варианты, которые лучше его по главному.

Список используемых источников

1. Советов Б. Я., Яковлев С. А. Моделирование систем: учеб. для вузов. 4-е изд., стер. М.: Высш. шк., 2005. 343 с.

2. Анисимов В. Г., Анисимов Е. Г., Осипенков М. Н., Селиванов А. А., Чварков С. В. Математические методы и модели в военно-научных исследованиях (в двух частях) / часть 1. М.: Военная академия Генерального штаба Вооруженных Сил Российской Федерации, 2017. 362 с.

УДК 004.056.5
ГРНТИ 50.37.23

ОБОБЩЕННЫЙ АНАЛИЗ РЕКОМЕНДАЦИЙ ПО КОНФИГУРИРОВАНИЮ СИСТЕМЫ БЕЗОПАСНОСТИ КЛАСТЕРА *KUBERNETES*

Г. В. Петров
Академия Федеральной службы охраны Российской Федерации

В статье представлены необходимые рекомендации, связанные с безопасностью кластера Kubernetes. Рассмотрены основные компоненты кластера Kubernetes. Определен ряд необходимых действий для обеспечения наибольшего уровня безопасности модулей оркестратора Kubernetes. Выделены подуровни конфигурирования сервисов безопасности Kubernetes. Сформулированы выводы в отношении построения информационных систем на основе кластера Kubernetes.

Kubernetes, контейнеры, DevOps, devsecops, обзор, безопасность.

Введение

Оркестратор *Kubernetes* является открытым программным обеспечением для автоматизации управления цифровыми услугами. Многие компании используют оркестратор *Kubernetes* для развертывания и управления своими сервисами в контейнерах. Разработчики отмечают преимущества, связанные с оперативностью и частотой развертывания новых версий приложений. Несмотря на данные преимущества, развертывание кластера *Kubernetes* подвержено ряду уязвимостей безопасности. Систематизация практик безопасности конфигурирования оркестратора *Kubernetes* может обеспечить уменьшение уязвимостей в развертывания кластера *Kubernetes*.

Цель этой статьи – предложить системный подход в обеспечение безопасности кластера *Kubernetes* посредством систематизации знаний, связанных с безопасностью кластера *Kubernetes*. Определен ряд мер безопасности, которые включают реализацию управления доступом на основе ролей, авторизацию для предоставления наименьших привилегий, применение безопасных модулей для обновления кластера *Kubernetes* и внедрением политик безопасности в структурный элемент узел и сетевых политик безопасности.

Систематизация имеющихся знаний о кластере *Kubernetes*, методы обеспечения безопасности могут обеспечить администрирующим лицам гарантию безопасности. Такая систематизация знаний может быть полезна для администраторов, которые хотят понять какие действия необходимо вы-

полнить для защиты кластера *Kubernetes* и могут использовать определенный список действий как эталон для сравнения состояния безопасности собственного кластера.

Представление основных модулей
и функций в структурной схеме кластера Kubernetes

На первоначальном этапе следует определить структурную схему кластера *Kubernetes*. Каждый кластер *Kubernetes* содержит набор рабочих машин, определенных как узлы. Как показано на рис. в кластере *Kubernetes* существует два типа узлов: мастер-узлы и рабочие узлы. Каждый главный узел включает в себя следующие модули: программного интерфейса приложения сервера (API – *Application Programming Interface*) «*API*-сервер», «планировщик», «контролер» и «*etcd*» [1]. Модуль «*API*-сервер» отвечает за организацию всех операций внутри кластера. Кластер *Kubernetes* выполняет свои функции через интерфейс прикладной программы «*API*-сервера». Модуль «контроллер» – это компонент на главном сервере, который следит за состояние кластера через «*API*-сервер» и изменяет текущее состояние к желаемому состоянию. Модуль «планировщик» – это компонент в плоскости управления, отвечающий за планирование развертывания контейнеров на нескольких узлах. Модуль «*etcd*» – это база данных по типу ключ и значение, в которой хранится вся информация о конфигурации для кластера *Kubernetes*. Пользователи используют инструмент командной строки *Kubectl* для связи с «*API*-сервером» на главном узле. На рабочих узлах размещаются приложения, работающие в кластере *Kubernetes* [1]. Следующие компоненты включены в рабочий узел: «*kube-proxy*», «*kubelet*» и «*pod*». Компонент «*kube-proxy*» поддерживает сетевые правила на узлах. Компонент «*kubelet*» – агент, который гарантирует, что контейнеры работают внутри модуля. Компонент «pod» наименьшая сущность кластера *Kubernetes*, включающая хотя бы один активный контейнер. Контейнер – это стандартный программный модуль, который упаковывает код и связанные зависимости для запуска в любом вычислительной среде.

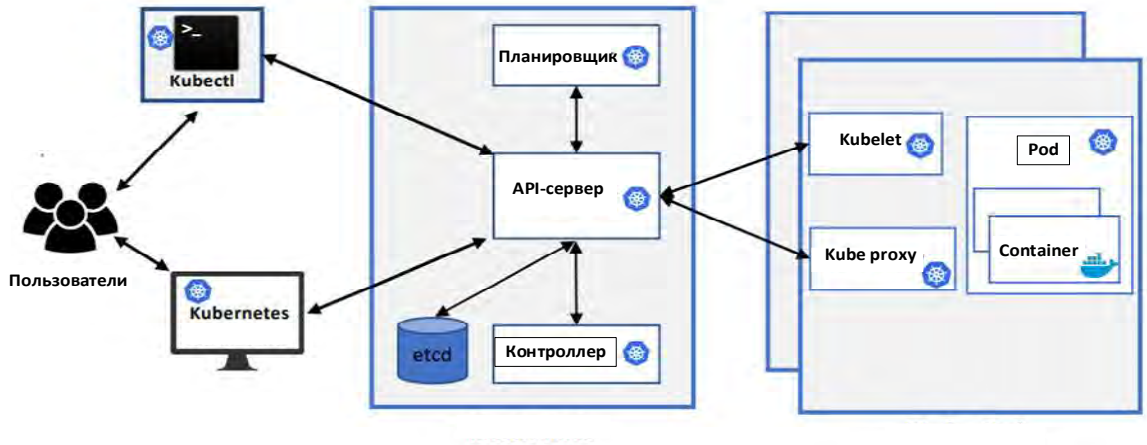


Рис. Структурная схема кластера Kubernetes

Необходимые сервисы безопасности
для реализации комплексной защиты кластера Kubernetes

Вследствие анализа основных модулей кластера *Kubernetes* определен перечень модулей и сервисов безопасности [2] требующих дополнительных конфигураций:

1. Аутентификация и авторизация;
2. Реализация специфичных для кластера *Kubernetes* политик безопасности;
3. Сканирование уязвимостей контейнеров приложений;
4. Логирование событий;
5. Разделение пространств имен;
6. Шифрование и ограничение доступа к *etcd*;
7. Постоянное обновление;
8. Ограничение квоты центрального процессора и памяти;
9. Использование протоколов *SSL/TLS*.

Аутентификация и авторизация

Существуют множество практик применения правил аутентификации и авторизации для предотвращения получения злоумышленниками доступа и выполнения несанкционированных действий. Аутентификация в кластере *Kubernetes* относится к аутентификации запросов «*API*-сервера» через плагины аутентификации. Авторизация в кластере *Kubernetes* относится к оценке каждого аутентифицированного запроса «*API*-сервера» относительно всех политик, разрешающих или отклоняющих запросы [3]. В ходе исследований особенностей реализации аутентификации и авторизации предложен перечень необходимых действий для оптимальной настройки:

1. Анонимный доступ к кластеру *Kubernetes* должен быть отключен. По умолчанию политика кластера *Kubernetes* разрешает анонимный доступ к «*API*-серверу».

2. Необходимо отключить режимы авторизации по умолчанию.

3. Конфигурации по умолчанию должны быть изменены. Использование конфигурации аутентификации и авторизации по умолчанию может позволить любой анонимный не аутентифицированный пользователь для выполнения несанкционированных действий.

Для аутентификации и авторизации рекомендовано использование протокола *OpenID* – стандартного протокола для системы децентрализованной аутентификации.

Реализация специфичных
для кластера Kubernetes политик безопасности

Реализация политик безопасности для определенных модулей кластера *Kubernetes* должна иметь комплексный подход в обеспечении безопасности всего кластера *Kubernetes* должна классифицироваться на следующие подсистемы:

1. Сетевые политики должны ограничивать сетевые запросы от нежелательных сетевых компонентов. Рекомендована установка надлежащих брандмауэров для блокировки нежелательных запросов с использованием плагинов сетевой политики, таких как *Calico* и настройка ограниченного доступа к базе данных для модулей.

2. Политики, специфичные для модуля «*pod*»: реализация политик к модулям и контейнерам. Рекомендовано запускать контейнеры внутри модуля должны без полномочий *root* с разрешениями только на чтение и включение модулей безопасности операционной системы *Linux*.

3. Общие политики: практика применения общих политик *RITY* для защиты компонентов кластера *Kubernetes* от внешних злоумышленников. Протокол управления передачей (*TCP – Transmission Control Protocol*) *TCP*-порты для кублета, *API*-сервера, *etcd*, сетевые плагины не следует оставлять открытыми и также данные компоненты должны требовать централизованной аутентификации.

Сканирование уязвимостей контейнеров приложений

Компоненты *Kubernetes*, такие как контейнеры, могут содержать уязвимости и вредоносное программное обеспечение. Если уязвимости присутствуют в контейнере, то вся система оркестрации подвержена атакам. Рекомендовано сканировать контейнеры на наличие уязвимостей с помощью таких инструментов, как *Dockscan 3* и *CoreOS Clair 4*.

Если образы и конфигурации развертывания не сканируются, тогда кластер *Kubernetes* уязвим для злоумышленников. Рекомендовано извлечение изображений из надежного частного реестра и проверка на уязвимости кода приложений и образов.

Логирование событий

Практики рекомендуют что ведение журнала должно быть включено для приложений, контейнеров внутри каждого модуля и для кластеров *Kubernetes* для проверки работоспособности системы. Без включения ведения журнала и мониторинга пользователи могут столкнуться с трудностями при устранении неполадок. Для внедрения практики логирования администраторам необходимо:

1. Контролировать журналы через регулярные промежутки времени.
2. Настроить оповещения при любых резких изменениях показателей журнала.

Разделение пространств имен

Создание отдельных пространств имен позволяет ресурсам быть изолированы между пространствами имен. Рекомендовано, чтобы каждое приложение в кластере должно иметь отдельное пространство имен для лучшей управляемости.

Шифрование и ограничение доступа к etcd

Применение практик шифрования и ограничения доступа к модулю «*etcd*», внутренним базам данных является надежным решением. Рекомендовано, чтобы модуль «*etcd*» был доступен только с модуля «*API*-сервера» и изолирован за брандмауэром, чтобы посторонние не могли получить доступ через *API*.

Постоянное обновление

Рекомендовано применять постоянные обновления кластера *Kubernetes*, а также проводят непрерывные обновления для развернутых приложений в модулях *Kubernetes*. Для постоянного обновления администраторам также рекомендуют использовать скользящие обновления, то есть установка *Kubernetes* патчи без нарушения доступности развернутых модулей приложения. В кластере *Kubernetes* существуют инструменты, такие как *kubectl* для выполнения скользящих обновлений.

Ограничение квоты центрального процессора и памяти

Практика ограничения центрального процессора и памяти модулем или пространством имен, чтобы уменьшить последствия атак. По умолчанию все ресурсы в кластере *Kubernetes* не имеют ограничений памяти и в доступе к процессору. Если злоумышленник начинает организацию атаки отказ в обслуживании, то из-за большого количества запросов, модуль «планировщик» создаст новый модуль и запустится экземпляр контейнера внутри нового узла. Этот процесс продолжается, пока он не использует все доступные

ресурсы центрального процессора и памяти. Следовательно, неспособность определить предела возможностей центрального процессора и ограничения памяти для модуля или пространства имен могут привести в потреблении всех доступных ресурсов в кластере *Kubernetes*.

Рекомендовано настроить количество ресурсов, определение максимального количества экземпляров для контейнера, количество ресурсов центрального процессора для приложения, и максимальный объем памяти для модуля или пространства имен.

Использование протоколов SSL/TLS

Возможна практика использования уровня защищенных сокетов (SSL – *Secure Sockets Layer*) или протокола безопасности транспортного уровня (TLS – *Transport Layer Security*) для обеспечения безопасной и зашифрованной связи между компонентами кластера *Kubernetes*. Включение протокола *TLS* между модулями кластера *Kubernetes* «*API*-сервером», «*etcd*», «*kubelet*» и «*kubectl*» обеспечивают безопасную связь связь между ними. Рекомендовано использование и обновление сертификатов *TLS* и *SSL* для модулей кластера *Kubernetes*.

Заключение

В результате проведения исследовательской деятельности представлен рекомендуемый список действий необходимых для обеспечения безопасности кластера *Kubernetes*. Анализ функционирования модулей кластера Kubernetes показывает, что эффективное и безопасное использование кластера *Kubernetes* требует разработки методов обеспечения безопасности, применимых к нескольким коммуникационным модулям в кластере *Kubernetes*.

Список используемых источников

1. Medium.Components of Kubernetes Architecture. URL: https://medium.com/-@kumargaurav1248/components-of-kubernetes-architecture-6feea4d5c712. (дата обращения 03.10.2020).

2. Marko Lukša Kubernetes in Action. Apress, 2018.

3. With Kubernetes, the U.S. Department of Defense Is Enabling DevSecOps on F-16s and Battleships, May 2020 URL: https://www.cncf.ro/case-study/dod/. (дата обращения 10.10.2020).

Сотрудник Академии ФСО,
кандидат технических наук И. А. Сенотрусов.

УДК 004.94
ГРНТИ 28.17.19

МЕТОДИКИ КОМБИНИРОВАННЫХ ИСПЫТАНИЙ КОММУНИКАЦИЙ ПРИОРИТЕТНЫХ ТРАНСПОРТНЫХ СРЕДСТВ С ПРИМЕНЕНИЕМ СИСТЕМЫ КОМПЬЮТЕРНОГО МОДЕЛИРОВАНИЯ

Я. А. Плетнев, А. В. Шестаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Исследуются пути снижения затрат на организацию испытаний сложных системотехнических решений на примере многослойных коммуникаций приоритетных транспортных средств посредством проведения комбинированных испытаний. Обосновывается методический аппарат многоцелевого применения методов и способов аналитического и имитационного моделирования на основе средств OMNET++, Veins, Plexe, SUMO для теоретических, экспериментальных исследований и испытаний сложных системотехнических решений. Критериальной основой в исследованиях принят требуемый уровень достоверности получаемых оценок характеристик существенных свойств системотехнических решений при различных условиях испытаний.

приоритетные транспортные средства, математическое моделирование, программа испытаний, методики комбинированных испытаний.

Введение

Одной из особенностей процедур теоретических и экспериментальных исследований системотехнических решений, конструкторско-технологических и программных решений коммуникаций приоритетных транспортных средств (СТР) является выбор и обоснование используемых методов и способов моделирования, которые непосредственно влияют на организацию проведения испытаний.

Проблемная область

Методы (способы) моделирования подразделяются на физические и математические, в т. ч. аналитические и компьютерные, которые содержат численные, статистические и имитационные методы. Физическое моделирование относится к натурным испытаниям транспортных средств, которые проводятся в реальных условиях использования коммуникационной инфраструктуры с оценкой характеристик существенных свойств многослойных коммуникаций по сформированной номенклатуре требований на основании

действующих нормативных и регламентирующих документов (рис. 1). В некоторых задачах, когда условия испытаний выполнить проблематично, могут использоваться иные методы моделирования, например, полунатурные или математические [1, с. 106–107]. Однако процедуры комплексирования различных методов моделирования существующими регламентами не определены, формальными способами для программ испытаний не описаны, с многослойностью коммуникаций не соотнесены.

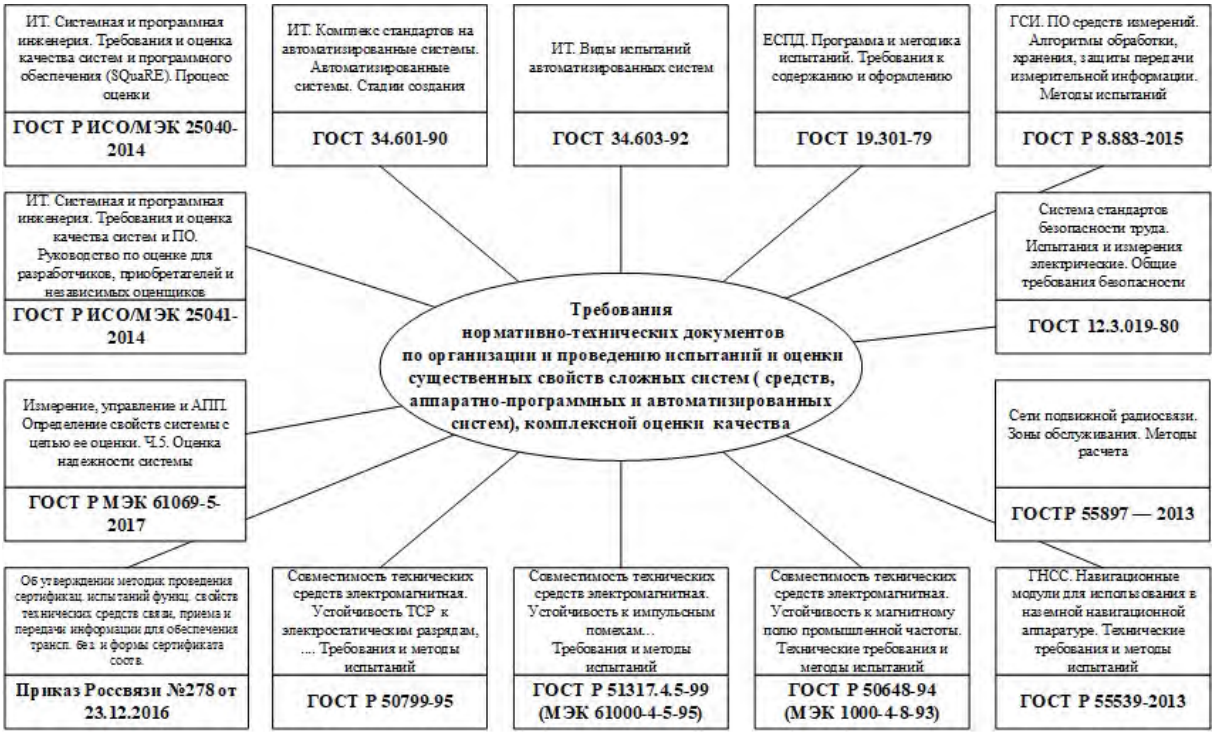


Рис. 1. Совокупность требований к организации,
проведению и оценке результатов испытаний коммуникационной инфраструктуры
и многослойных коммуникаций

Результаты

Организация испытаний отражена в программе испытаний, организационно-методическом документе, разделы которого (объект, цели, виды, последовательность, объем, порядок, условия, место, сроки, отчетность) и содержание регламентированы. Испытания коммуникаций приоритетных транспортных средств, в части характеристик существенных свойств СТР попадают под требования нормативно-технических документов по организации и проведению испытаний для сложных коммуникационных систем, радиоэлектронных средств и навигации, а процедуры оценки качества СТР – к измерению и оценке качества компьютерных систем, информации и качества при использовании (рис. 2-3 по ГОСТ Р ИСО/МЭК 25040).

Рис. 2. Процедуры измерений

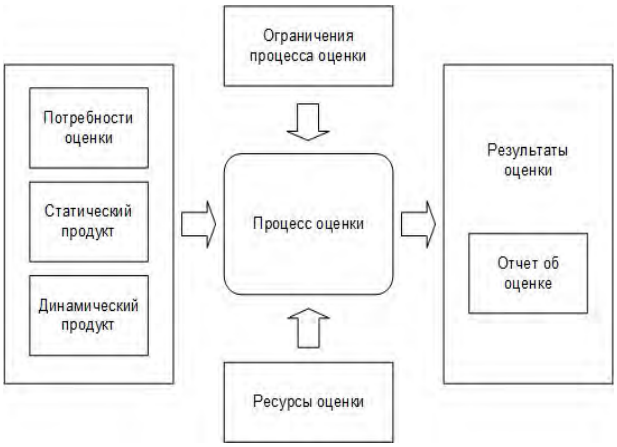


Рис. 3. Процедуры оценки

Сложность процедур частных методик по программе испытаний коммуникаций транспортных средств – в моделировании, например, в условиях интенсивной городской среды, которые реализуются программными средствами с привязкой к ГИС-региона (рис. 4–9) [2].

Рис. 4. Невский район, Санкт-Петербург (скрин-шот)

Рис. 5. Модельная ситуация: Невский район, Санкт-Петербург (скрин-шот)

Рис. 6. Петроградская сторона, Санкт-Петербург (скрин-шот)

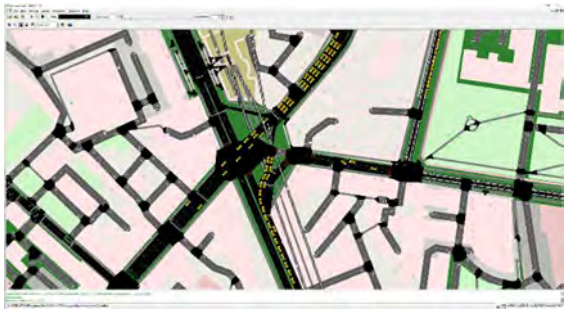


Рис. 7. Модельная ситуация: Петроградская сторона, Санкт-Петербург (скрин-шот)

Сложность моделирования многослойности коммуникаций с учетом требуемой послойной адекватности результатов также возрастает. Принятая для приоритетных транспортных средств концептуальная модель многослойных коммуникаций соотнесена с компонентами модели интеллектуальной транспортной системы [2]. Концептами многослойных коммуникаций приоритетных транспортных средств выступают структурные функциональные параметры, информационные компоненты, внешние и внутренние условия, влияющие на основные характеристики коммуникаций. Концептуальная модель позволяет сформировать требуемую конфигурацию платформенных средств имитационного моделирования, таких как OMNET++, Veins, Plexe, SUMO и других подобного типа, под различные условия и задачи по программе испытаний [3].

Методики комбинированных испытаний СТР с применением системы компьютерного моделирования должны учитывать требуемый уровень достоверности получаемых оценок, т. е. содержать решающие правила перехода не только к математическому моделированию, но и к послойным испытаниям многослойности коммуникаций.

Обсуждение

Методики комбинированных испытаний коммуникаций приоритетных транспортных средств с применением системы компьютерного моделирования, как вспомогательного процесса испытаний СТР, содержат процедуру (блок 6 рисунок 8) перехода к математическому моделированию (при необходимости) [4].

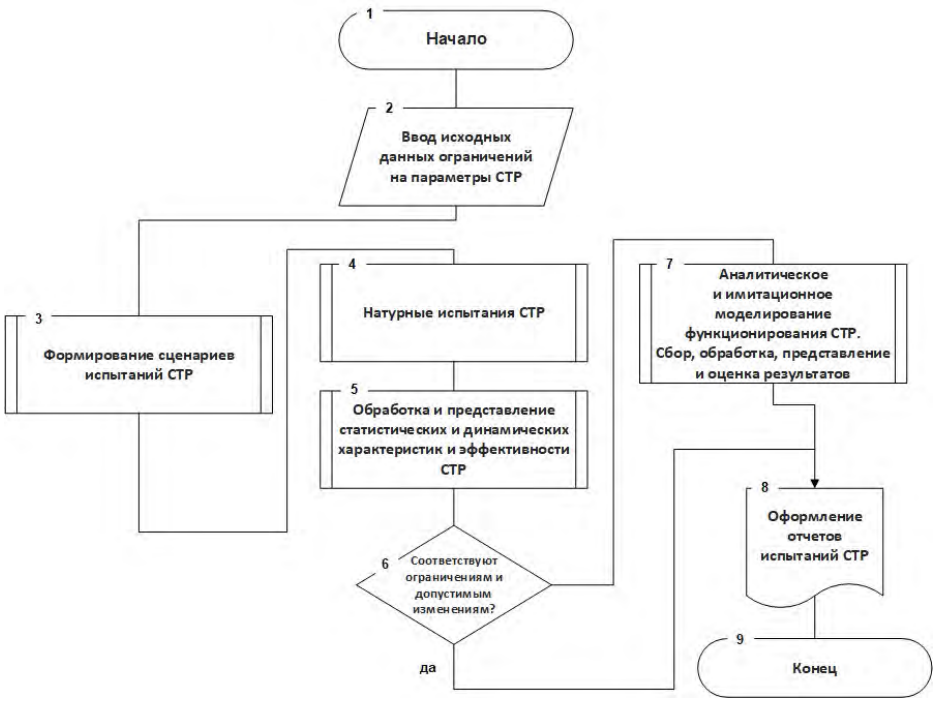


Рис. 8. Методика испытаний с ограниченным компьютерным моделированием

Методика испытаний СТР с ограниченным компьютерным моделированием для детализации коммуникаций содержит совокупность процедур послойного моделирования (блок 7 рис. 8).

Методика комбинированных испытаний СТР на общий случай (рисунок 9) включает процедуры определения объемов (блок 3), порядка и условий (блоки 6.1-6.3) компьютерного моделирования.

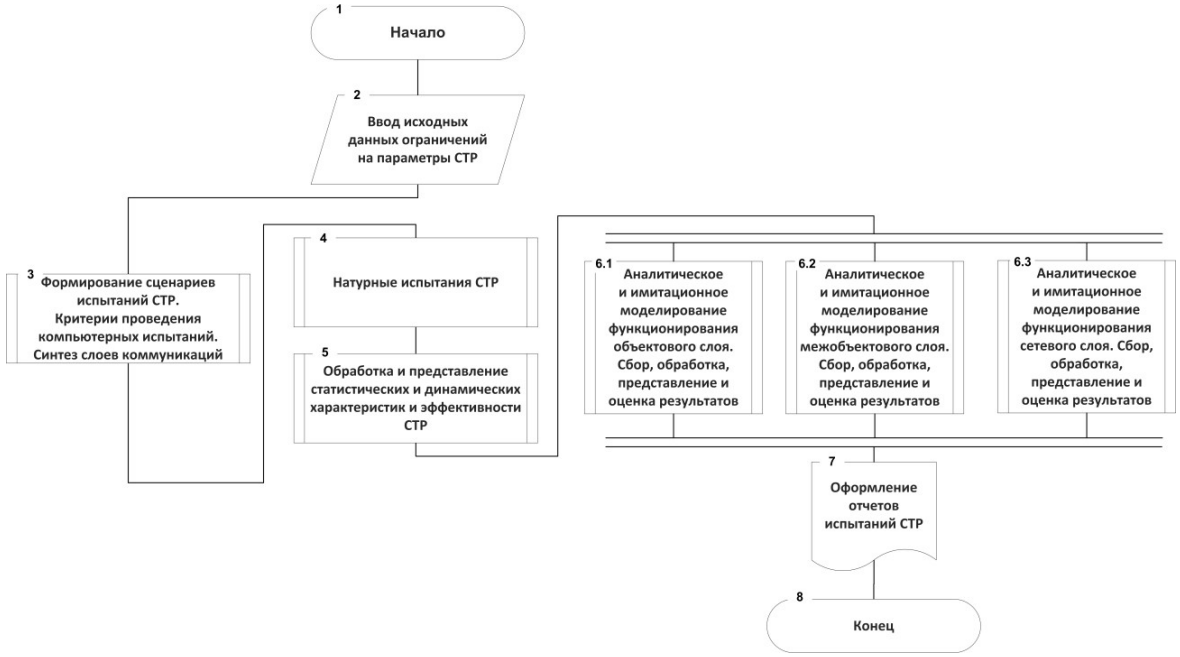


Рис. 9. Методика испытаний с компьютерным моделированием

Снижение затрат на организацию испытаний посредством применения предложенных методик приведено на рис. 10.

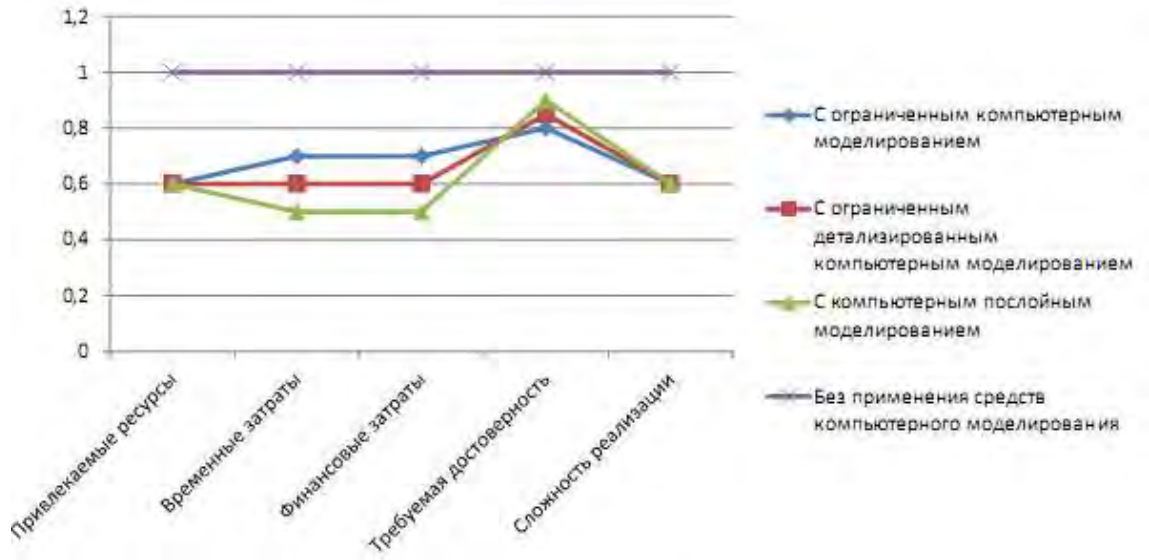


Рис. 10. Результаты оценки применения комбинированных методик

Методики комбинированных испытаний коммуникаций приоритетных транспортных средств являются результатом решения методических проблем организации и проведения испытаний сложных СТР к которым относятся: структурно-параметрическая сложность СТР; значительная вариативность СТР; неявная многокритериальность при выработке конструкторско-технологических и программных решений; неопределенность в степени и уровне влияния внешних воздействующих условий и факторов с учетом их изученности для объекта исследования.

Заключение

Предложенный методический аппарат можно реализовать на практике без доработки, что позволит существенно сократить временные и финансовые затраты на получение полного набора данных о результатах испытаний сложных системотехнических решений.

Список используемых источников

1. Шестаков А. В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. СПб.: ГУАП, 2016. 325 с.

2. Плетнев Я. А., Шестаков А. В. Концептуальная модель многослойных коммуникаций приоритетных транспортных средств // Сб. трудов конф. VI Всеросс. научно- технич. конф. "Цифровая экономика. Новое время - Новые технологии. РОСИНФОКОМ 2020", 18.11.2020. Самара: ПГУТИ, 2020. С. 35–36.

3. Pletnev, Y. A.; Frolova, K. A.; Shestakov, A. V. Data Updating Models for Priority Vehicles // 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Brno, Czech Republic, 2020. Pp. 325–330, doi: 10.1109/ICUMT51630.2020.9222414.

4. Отчет по 2 этапу НИР «Приоритетный проезд» (промежуточный) Регистрационный номер Сведений о результатах НИОКТР в БД ЕГИСУ НИОКТР: АААА-Б20-220122490081-9 от 24.12.2020, раздел 2.

УДК 654.739
ГРНТИ 49.33.29

РОЛЬ SEO И ДИЗАЙНА САЙТА В СФЕРЕ ПОИСКОВОГО ПРОДВИЖЕНИЯ

О. П. Погадаева, А. А. Шиян

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Методы поисковой оптимизации веб-ресурсовиграют важную роль в выведении сайта в топ поисковых запросов. В статье проводитсясравнительное исследование сайтов СПбГУ, СПбГУП, СПбГУТ и опрос 150 респондентов (по 50 от каждого университета). Рассматриваются наиболее важные факторы, которые влияют на позиционирование веб-страницы в результатах поиска.

SEO-продвижение, веб-дизайн, веб-сайт, сайты университетов Санкт-Петербурга, визуальная коммуникация, метод контент-анализа.

Поисковые системы играют важную роль в продвижении. Методы поисковой оптимизации (SEO), должны вести к первым позициям в результатах поиска. По мере того, как Интернет и веб-дизайн динамично развиваются, новые методы оптимизации процветают и терпят поражение. Основное внимание в этом исследовании уделяется установлению того, могут ли визуальный контент и эстетика повлиять на решение студентов рассмотреть вопрос о поступлении в какой-либо конкретный университет. Мы рассмотрели наиболее важные факторы, которые могут помочь улучшить позиционирование в результатах поиска. Далее мы представили и изучили объект оптимизации, которым является конкретный веб-сайт. Основная цель этой статьи состояла в том, чтобы определить, увеличивает ли поисковая оптимизация рейтинг веб-сайта в результатах поиска и, соответственно, приводит ли к увеличению трафика.

Рынок, на котором работают высшие учебные заведения, характеризуется растущей конкурентной средой среди университетов с целью информирования, напоминания и убеждения потенциальных абитуриентов выбирать и применять свои программы на получение степени [1]. Более того, будущие студенты, составляющие целевой рынок высших учебных заведений, характеризуются навыками работы в Интернете с хорошими коммуникативными навыками, более информированными и подготовленными к принятию решений [2]. Это подчеркивает важную роль SEO-продвижения в привлечении и удержании студентов и его общую значимость в секторе высшего образования.

Проведено исследование сайтов университетов Санкт-Петербурга. Предмет анализа – лидеры поисковой выдачи по запросу: «Сайты университетов Санкт-Петербурга». К конкретным университетам относятся Санкт-Петербургский государственный университет (СПбГУ), *Санкт-Петербургский университет* профсоюзов (СПбГУП) и Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича (СПбГУТ). Определив университеты с самой большой видимостью в поиске, можно начать анализировать, что позволяет им эффективно получать трафик поисковых систем.

Исследование позволило выявить много общего между веб-сайтами проанализированных университетов. Большинство веб-сайтов содержали большие фотографии студентов, мест и людей, чтобы информировать потенциальных абитуриентов и аудиторию о своих предложениях. Кроме того, все они имели один или два уровня первичной навигации по меню веб-сайта со знакомым содержанием, которое включает типы программ на получение степени, способы подачи заявки, контактную информацию и многое другое. Два из веб-сайтов включали календарь событий, занимающий видное место на веб-сайте университета. FQA и отзывы студентов также были частью популярных стратегий веб-сайтов среди университетов. В целом, университеты использовали различные вербальные, визуальные и интерактивные компоненты на своих веб-сайтах, чтобы сообщить о своих предложениях и процессе межкультурной компетенции.

Для дальнейшего изучения веб-сайтов СПбГУ, СПбГУП, СПбГУ был использован метод контент-анализа. В этом исследовании респонденты, в состав которых входили студенты из каждого из выбранных университетов, составляли целевую группу.

Опрос проводился в дистанционном формате с использованием инструмента Google Формы. Выборка включала 150 респондентов (по 50 от каждого университета). Все 150 респондентов ответили и вернули свои анкеты, что составило 100 % ответов.

Исследование выявило много общего между тремя анализированными сайтами университетов. Все веб-сайты содержали большие фотографии студентов, мест, людей и даже отзывы студентов, чтобы привлечь потенциальных клиентов к этому учебному заведению. Вдобавок у всех было по два и более уровней первичной навигации через раздел «Соискатель» на веб-сайте с аналогичным содержанием, включая программы бакалавриата, студентов по обмену, подачу заявок, руководство для новых студентов, истории студентов и многое другое. СПбГУ разместил календарь событий на видном месте на своей домашней странице. Часто задаваемые вопросы (FAQ) СПбГУП и СПбГУТ также являются частью популярных стратегий двух университетов. В целом, кейс-университеты имели на своих веб-сайтах множество вербальных, визуальных и интерактивных компонентов.

Следующие вопросы были основными вопросами, которые нужно было изучить и проанализировать. Во-первых, учащихся спросили, какой имидж на веб-сайте университета был представлен им об университете во время периода подачи заявок в университет. Во-вторых, был ли веб-контент на домашней странице учебного заведения достаточно убедительным, чтобы повлиять на их выбор. И последнее, если таковая имеется, какая информация из веб-контента учреждения оказала наибольшее влияние на то, когда они решили подать заявление о приеме и оценить важность этой информации. Их также попросили оценить факторы по шкале от 1 до 5, где 1 означает «совсем не важно» и 5 «очень важно». Данные опроса представлены на рис. 1-3.

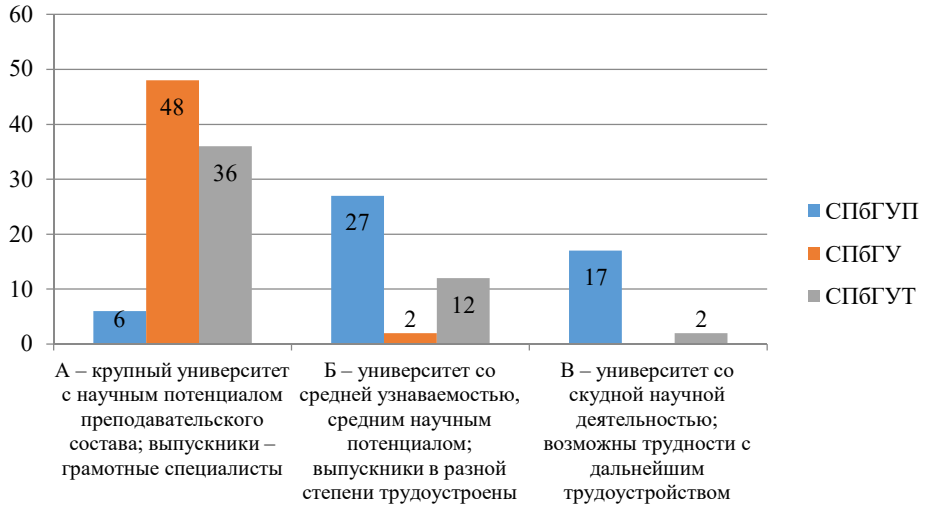


Рис. 1. Какое впечатление сложилось об университете во время периода подачи документов

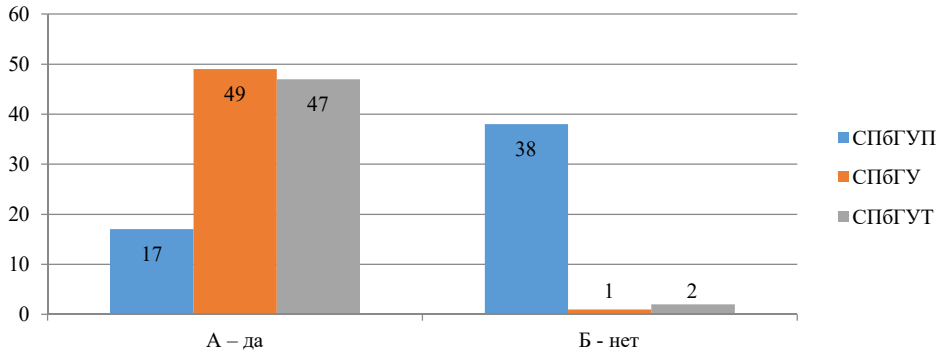


Рис. 2. Повлиял ли вид главной страницы университета на ваш выбор

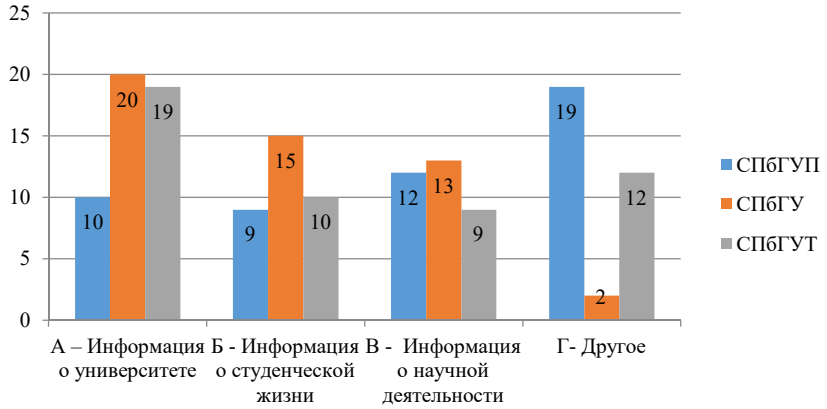


Рис. 3. Какая информация оказала наибольшее влияние на решение абитуриента

Ответов участников было много, однако ответы с похожим содержанием были сведены в один. Ответы можно разделить на две основные категории: содержание веб-сайта, другие контакты с университетом. Из 150 участников 116 заявили, что веб-сайт университета был их первой точкой контакта с учреждением, поскольку у них не было предыдущих контактов или рекомендаций от кого-либо, чтобы повлиять на выбранный ими университет. Некоторые респонденты заявили, что легкость доступа к информации и навигации по ней в сочетании с отзывами студентов на домашних страницах вуза является положительным определяющим фактором для их выбора.

Проведенное исследование позволило сделать вывод, что для выведения сайта к первым позициям в результатах поиска нужно обращать внимание на все: чем больше разных закономерностей будет выявлено, тем выше шансы проекта соответствовать требованиям поисковиков и быть полезным для пользователя. Повлиять на успех может как содержимое отдельной страницы, так и структура, удобство навигации по сайту в целом.

Часто разработка дизайна выстраивается линейно, главная страница позиционируется как первый этап. В действительности же значительная часть органического трафика инициируется внутренними страницами [3]. SEO позволяет рассмотреть реальные сценарии взаимодействия пользователя ссайтом, положительно влияя на поведенческие показатели. Это благоприятно скажется на его дальнейшем продвижении [4].

Проведенное исследование показывает, что SEO-оптимизация и дизайн страниц оказывают глубокое влияние на восприятие пользователей представленной информации веб-ресурсов.

Растущий интерес к измерению степени использования университетами своих веб-сайтов свидетельствует о растущем значении, которое университеты придают своим веб-сайтам. При разработке сайта важно выбрать подходящий контент, визуальные элементы и эстетику, которые обеспечи-

вают двойную пользу: донесение правильного сообщения до нужной аудитории, а также создание прочной и эмоциональной связи с пользователями. Важно отметить, что каким бы визуально привлекательным ни казался университетский веб-сайт, чрезмерное использование графики и разрозненной информации может запутать потенциальных студентов и привести к потере интереса. Поэтому для привлечения потенциальных студентов необходимо сохранять простой дизайн с соответствующим использованием изображений и связанной с ними информации, которая должна быть хорошо организована, наряду с удобной системой навигации. Один из лучших способов сохранить для потенциальных абитуриентов наилучшее качество подачи заявок на поступление – это разработать веб-сайты так, чтобы они обладали необходимой информацией, чтобы эти группы могли легко использовать сайт, находить информацию и получать доступ к помощи там, где это необходимо. Содержание веб-сайта должно быть четким, хорошо написанным, без ошибок, и пользователь должен видеть, как перемещаться по сайту.

Также должны быть предприняты усилия по улучшению веб-контента, чтобы охватить как официальную информацию, так и информацию из повседневной жизни. На веб-сайтах этих университетов должна быть представлена очень важная повседневная информация, такая как информация об услугах здравоохранения, принимающем сообществе, социальных сетях, стоимости обучения, стипендии, возможностях программы обмена и т. д.

Таким образом, в этом исследовании делается вывод о том, что университету (СПбГУТ) следует улучшить архитектуру и содержание своего веб-сайта. Это сделает веб-сайт хорошим инструментом коммуникации, тем самым выведя сайт к первым позициям в результатах поиска. Это не только повысит удобство использования и видимость веб-сайта, но и поможет донести правильное представление об университете до потенциальных абитуриентов и других заинтересованных сторон, тем самым поможет продвигать университет и, в конечном итоге, увеличить количество учащихся.

Список используемых источников

1. Plamer, O. Web site usability, design, and performance metrics // Journal of Information Systems Research. 2002. № 13 (2). Pp. 151–167.

2. Poock, E. Characteristics of an effective web site in educational leadership // College Student Journal. 2006. № 40 (4). Pp. 785–790.

3. Matusitz, R. The Current Condition of Visual Communication in Colleges and Universities of the United States // Journal of Visual Literacy. 2005. № 25 (1). Pp. 97–112.

4. Braddy, W.; Wuensch, L. Internet recruiting: The effects of web page design features // Social Science Computer Review. 2003. № 21. Pp. 374–385.

УДК 004.021
ГРНТИ 28.27.19

ПОИСК ИСХОДНЫХ СОБЫТИЙ ДЛЯ ОЦЕНКИ БЕЗОПАСНОСТИ ОПЕРАЦИЙ ПО ПЕРЕГРУЗКЕ ЯДЕРНОГО ТОПЛИВА

В. О. Попова[1], **А. А. Чечулин**[1,2]

[1]Университет ИТМО
[2]Санкт-Петербургский федеральный исследовательский центр Российской академии наук

В настоящей статье рассматривается формализованный подход для выявления исходных событий, которые могут привести к авариям при перегрузке ядерного топлива. Данный подход позволит сформировать список необходимых и достаточных мер защиты от аварий, а также определить избыточность в защитных мерах и выявить аварийные ситуации, меры защиты для которых не предусмотрены.

методы анализа безопасности, метод HAZOP, перегрузка ядерного топлива, канальные реакторы большой мощности (РБМК).

В настоящее время в нашей стране, в основном, эксплуатируется два типа реакторных установок: водо-водяные энергетические реакторы (ВВЭР) и канальные реакторы большой мощности (РБМК). Два типа реакторов имеют принципиальные отличия с точки зрения основных принципов работы [1, 2]. Актуальность выбранного вопроса, а именно, безопасность операций по перегрузке ядерного топлива (РБМК), связана с особенностями эксплуатации блоков РБМК. Одним из самых опасных, с точки зрения аварийности на современных АЭС, является процесс перегрузки ядерного топлива. Во время проведения операций по перестановке топливных кассет существует риск повреждения топлива, и, как следствие, вероятность выхода радиоактивных веществ за допустимые пределы. Перегрузка топлива на реакторах типа РБМК происходит, в том числе, во время нахождения реактора на мощности (в среднем происходит замена 2–3 кассет в сутки), в отличие от ВВЭР, где для этого реактор останавливают, что делает процесс перестановки кассет на РБМК еще более опасным. Процесс перегрузки РБМК при нахождении реактора на мощности состоит из очень большого количества сложных операций, характеризующихся множеством параметров. Несоблюдение критериев выполнения операций, выход значений параметров за допустимые диапазоны с большой вероятностью может привести к аварии.

Для повышения безопасности и уменьшения вероятности повреждения топлива реализуются меры для предотвращения подобных инцидентов. В настоящее время в практике эксплуатации АЭС такие меры формируются

на основе методов анализа безопасности технически сложных систем. Однако, большинство методов анализа безопасности технически сложных систем основано на том, что возможные виды отказов оборудования или опасные отклонения формируются на основе знаний и опыта эксперта. В некоторых случаях такой подход вносит существенный субъективизм в результаты анализа безопасности. Для уменьшения субъективизма при выполнении анализа безопасности и формализации процедуры определения исходных событий могут использоваться различные методы классификации. Например, для компьютерной инфраструктуры могут использоваться существующие классификации атак [3]. В настоящем исследовании для более обобщенного решения этой задачи предлагается использовать метод HAZOP (англ. *HAZard and OPerability*, рус. Опасность и Работоспособность). Метод HAZOP [4] был разработан в 60-ые годы прошлого века и представляет собой описание процесса поиска и описания опасных состояний оборудования и причин, приводящих к таким состояниям. В основу метода HAZOP положено понятие «путь изменения» и «наводящее слово». Под путем изменения понимается физическое перемещение механизмов оборудования от точки А к точке В или переход от одного состояния к другому (рис.).

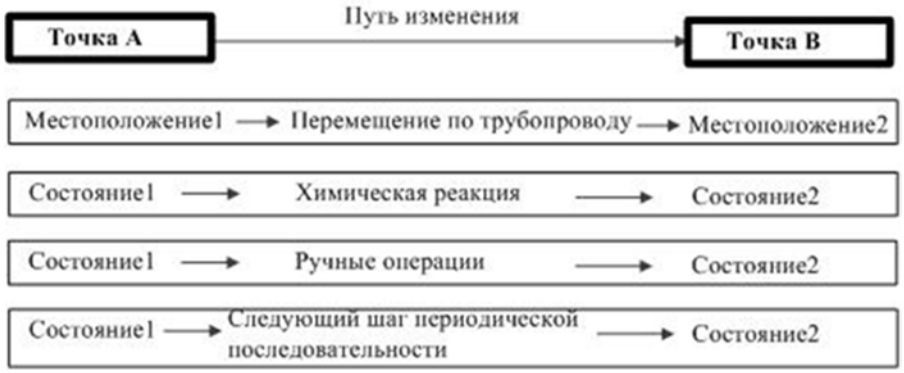


Рис. Понятия о пути изменения

Наводящее слово – слово или группа слов позволяющие стимулировать поиск возможных отклонений параметров технологического процесса на каком-либо конкретном пути изменения. Примеры наводящих слов и их значений приведены в таблице 1 [5].

ТАБЛИЦА 1. Пример наводящих слов и их значения

Наводящее слово	Значение
НЕТ (или НИЧТО)	Ни одна из целей проекта не достигнута
БОЛЬШЕ (более, выше)	Количественное увеличение
МЕНЬШЕ	Количественное уменьшение
ТАКЖЕ КАК (более чем)	Происходит качественное изменение

Наводящее слово	Значение
	или дополнительная работа
ЧАСТЬ (чего-либо)	Только некоторые из целей проекта достигнуты
ВОЗВРАТ	Логически противоречит целям проекта
ИНОЕ	Полная замена – имеет место другая работа
ГДЕ ЕЩЕ	Относится к потокам, переходам, источникам, местам назначения
ДО / ПОСЛЕ	Относится к порядку последовательности
РАНО / ПОЗДНО	Временные оценки, отличающиеся от ожидаемых
БЫСТРЕЕ / МЕДЛЕННЕЕ	Шаг выполнен быстрее или медленнее, чем было намечено

Сочетание наводящих слов с конкретными параметрами оборудования, характерными для рассматриваемого пути изменения, позволяют генерировать возможные отклонения в состоянии оборудования (табл. 2).

ТАБЛИЦА 2. Наводящие слова, примененные к параметрам процесса и позволяющие описать реальные отклонения [4, 5]

Параметр оборудования	Наводящие слова, способные дать имеющую смысл комбинацию
Расход (поток)	Не больше, чем; меньше, чем; возврат; где-то; также, как.
Температура	Выше, ниже
Давление	Выше, ниже, вакуум
Уровень	Нет, выше, ниже
Смещение	Меньше, больше, никакого
Реакция	Выше (скорость), ниже (скорость), отсутствует, обратная; такая же, как
Фаза	Другая, обратная; такая же, как.
Состав	Часть; такой же, как.
Передача информации	Нет, часть, больше, меньше, иная; такая же, как.

В рамках исследования, была осуществлена адаптация метода HAZOP применительно к РЗМ. Разгрузочно-загрузочная машина (РЗМ) предназначена для перегрузки реактора РБМК.

Анализ HAZOP для к РЗМ включает решение следующих задач.

Задача 1. Анализ технологических операций, выполняемых с использованием РЗМ, определение состояние РЗМ и возможных путей изменения. При определении состояний РЗМ необходимо придерживаться следующих правил:

– неизменность физических параметров системы (давление, температура и т. д.);

– неизменность состояния механизмов в части наличия движения;

– неизменность состояния системы в части заданных оператором параметров и режимов управления.

При изменении текущего состояния система переходит в следующее состояние, характеризующееся путем изменения. При определении возможных путей изменения необходимо придерживаться следующих правил.

Переход РЗМ из одного состояния в другое характеризуется плавным или скачкообразным изменение одного или нескольких параметров. В рамках анализа HAZOP нужно стремится к тому, чтобы рассматривать как можно более короткие пути изменения. В общем случае рекомендуется рассматривать пути изменения, связывающие соседние в порядке выполнения технологического процесса состояния. Пример возможных путей изменения состояния РЗМ:

– перемещение моста, тележки на гнездо тренажерного стенда (ТС);
– стыковка с гнездом ТС;
– поворот пустого магазина;
– перемещение пустого захвата вниз;
– отвинчивание пробки;
– перемещение захвата со свежим топливом вверх
– расстыковка с каналом.
– перемещение пустого захвата вниз и захватывание кассеты
– отвинчивание пробки (разгерметизация ТК) и т. д.

Задача 2. Анализ путей изменения и формирование возможных отклонений. Для решения этой задачи предлагается сгруппировать параметры и определить характерные отклонения для них. В общем случае набор параметров РЗМ должен быть разбит на группы. Например, группа «Давление» включает давление в скафандре, барабан-сепараторах и в канале реактора. Анализ условий работы РЗМ позволил выделить для каждой группы параметров характерные и наиболее опасные отклонения (табл. 3).

ТАБЛИЦА 3. Возможные отклонения параметров

Группа параметров	Возможные отклонения
Давление	Превышение допустимого значения, отсутствие изменения, отклонение от заданного
Усилие	Несоответствие заданному состоянию захвата, превышение допустимого значения
….	...

Задача 3. Представление результатов в виде таблицы (табл. 4).

ТАБЛИЦА 4. Сводная таблица с результатами

Путь изменения	Возможные отклонения	Последствия отклонений
Отвинчивание пробки (разгерметизация ТК)»	Несанкционированное опорожнение стыковочного патрубка (падение давления в стыковочном патрубке)	Нарушение баланса давления в канале и стыковочном патрубке может привести к повреждению кассеты и РЗМ
Перемещение захвата с отработавшим топливом вверх	Несанкционированное увеличения усилия на захвате	Повреждение кассеты в результате «затирания» в канале
….	…	…

На современных блоках РБМК в системах автоматического управления РЗМ предусмотрено порядка 63 технологических операций, которые позволяют осуществить процесс перегрузки. Такие операции состоят из множества действий с большим количеством параметров. Адаптация метода HAZOP применительно к РЗМ позволила систематизировать поиск исходных событий, приводящих к нежелательным событиям и, как следствие, позволяет оптимизировать защитные меры, что приводит к повышению надежности работы системы, упрощает процесс эксплуатации и может уменьшить время рабочего цикла контроллера на обработку защитных мер.

Работа выполнена при частичной финансовой поддержке РФФИ (проект 19-29-06099 мк).

Список используемых источников

1. Родионов В. Г. Энергетика: проблемы настоящего и возможности будущего. М.: ЭНАС, 2010. 352 с.

2. Аветисян А. Р., Пащенко А. Ф., Пащенко Ф. Ф., Пикина Г., Филиппов Г. Теплогидравлические модели оборудования электрических станций. М.: ФИЗМАТЛИТ, 2013. 448 с.

3. Котенко И. В., Дойникова Е. В., Чечулин А. А. Общее перечисление и классификация шаблонов атак (CAPEC): описание и примеры применения // Защита информации. Инсайд. 2012. № 4. С. 54–66.

4. Trvor Kletz. HAZOP and HAZAN. Rugby: IChemE, 2006. 256 p.

5. Макдональд Д., Хвилевицкий Л., Серебрянский А. Промышленная безопасность, оценивание риска и системы аварийного останова. М.: Группа ИДТ, 2007. 416 с.

УДК 004.056(075.8)
ГРНТИ 81.96

АНАЛИЗ СИСТЕМЫ ГОЛОСОВАНИЯ В РЕСПУБЛИКЕ ИРАК И ПУТИ ПЕРЕХОДА К СИСТЕМЕ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

В. Д. Салман

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Проводится анализ системы голосования в Республике Ирак и исследуются основные проблемы, связанные с ее эксплуатацией. Проведенный анализ показал, что существующая система голосования имеет проблемы с безопасностью и нуждается в модернизации с использованием информационно-коммуникационных технологий с целью ее соответствия мировым стандартам. Сделан вывод о необходимости применения онлайн-голосования на иракских выборах, обеспечивающего новую систему доверия и безопасности для пользователя и правительства Ирака. Дополнительным преимуществом такой системы является возможность избирателей голосовать в любое время в любом месте через интернет.

система голосования, система голосования в республике Ирак, электронное голосование, онлайн-голосование.

Голосование – это инструмент, используемый избирателем для свободного выражения своего мнения на выборах.

В Ираке, первые демократические выборы состоялись в 2005 году, после годичного периода оккупации. Эти выборы, проведенные независимой избирательной комиссией Ирака (IECI), были основаны на пропорциональном представительстве по закрытому списку и традиционной бумажной системе голосования [1].

Голосование с использованием бумажных бюллетеней имеет существенные недостатки: очень дорогое, долго подсчитывается результат голосования, возможна манипуляция и фальсификация результатов, инвалиды и пожилые люди не всегда могут прийти на избирательные участки для голосования. Исходя из этого делаются попытки решить проблемы голосования с помощью информационно-коммуникационных технологий. Одним из видов электронного голосования является система онлайн-голосования. Система позволяет избирателю отдать свой голос из любого места и в любое время через Интернет.

Амин Зина [2], предложил веб-приложение, заменяющее традиционный бумажный процесс голосования. Данное веб-приложение использует

ASP.net, с помощью SQL сервера реализует процесс голосования на избирательном участке и выдает результаты выборов. Система устанавливается на одином или нескольких компьютерах на избирательного участка, который, в свою очередь отвечает за вход избирателя в систему с именем пользователя и секретным паролем, а также установку системы, которая может работать непрерывно в течение разрешенного периода процесса голосования. Недостатки этой системы: избиратель должен посетить избирательный участок, чтобы отдать свой голос, а также то, что система не удовлетворяет требованиям безопасности в полной мере.

Табра Ясмин М. [3] предложила систему онлайн - голосования для Ирака. Система очень проста и удобна в использовании, а также создает и управляет деталями голосования и выборов; поскольку все избиратели должны войти в систему, введя свою проверенную информацию и пароль, а затем выбрать своих кандидатов. Система разработана с использованием нескольких языков программирования, таких как HTML, JavaScript, CSS, PHP, MySQL. Однако в полной мере в данной системе требования безопасности не удовлетворяются, поскольку не используются современные алгоритмы шифрования и она легко взламывается.

Джафар Халид и др. [4] разработали систему онлайн - голосования на выборах в Ираке. Система включает: панель входа, регистрацию избирателя, администратора. Избиратель должен войти на страницу регистрации для удостоверения личности. При голосовании, избиратель должен ввести имя пользователя, после чего откроется окно входа для избирателя, где вводятся идентификатор избирателя и пароль. Недостатком этой системы является то, что администратор системы может видеть весь процесс голосования. Эта система не обеспечивает безопасное соединение между браузером избирателя и сервером голосования.

Система электронного голосования должна удовлетворять следующим требованиям: аутентификация, уникальность, точность, целостность, тайна голосования и подтверждение голоса.

Таким образом, ни одна из предложенных систем электронного голосования не удовлетворяет в полной мере мировым стандартам on-line голосования.

Главным органом избирательной системы Ирака является Независимая Высшая Избирательная Комиссия Ирака (IHEC). Это независимый избирательный орган, состоящий из девяти членов, назначаемых Советом представителей (CoR) и находящихся под его наблюдением. Основные функции IHEC определены в законе IHEC № 11 от 2007 года: создание и обновление регистрации избирателей; регистрация и аттестация партий для участия в выборах; регулирование и удостоверение списков кандидатов на выборах; аккредитация наблюдателей, представителей партий и средств массовой информации; рассмотрение всех избирательных жалоб и апелляций (могут

быть обжалованы только в специальной судебной избирательной коллегии); удостоверение процедуры подсчета голосов; объявление и удостоверение результатов выборов и референдумов; установление нормативных актов и инструкций по обеспечению справедливого избирательного процесса, удостоверение структуры и назначение руководящего состава избирательной администрации; установление финансовой политики для IHEC [1, 5].

Проблемы, с которыми сталкивается IHEC в существующей иракской системе голосования: запугивание или подкуп сотрудников IHEC или избирателей, фальсификация, подрыв тайны голосования, кража или уничтожение любого из ящиков для голосования, а также изменение голосов [1].

Избирательная система Ирака представляет собой пропорциональную систему представительства провинций и состоит из 329 мест. Женщины должны составлять не менее 25 % членов парламента. Голосование не является обязательным. Избиратели, имеющие право голоса, имеют иракское гражданство, возраст не менее 18 лет, зарегистрированы в списке избирателей, имеют электронную карту и удостоверение личности с фотографией или биометрическую карту избирателя. Легитимные кандидаты имеют иракское гражданство, возраст не менее 30 лет, имеют свидетельство об образовании и не должны быть судимы [5].

В 2018 году IHEC использовала на выборах технологию биометрической регистрации и верификации, а также впервые использовала технологию подсчета и передачи результатов с избирательных участков в центры подсчета голосов IHEC в день выборов. Иракская система голосования состоит из следующих этапов:

Регистрация. Регистрация всех имеющих право голоса избирателей в базе данных избирателей и обновление информации об избирателях. Биометрическая регистрация избирателей проводилась в период с июня 2014 года по 9 ноября 2017 года. Биометрическая карта избирателя [5] – изображена на рис. 1.

Рис. 1. Биометрическая карта

Рис. 2. Избирательный бюллетень

Голосование. Выборы проходили в один день с 7:00 утра до 6:00 вечера. На каждом избирательном участке были копии списков избирателей и электронные устройства для идентификации избирателей. Избиратель перед голосованием, должен был расписаться в списке избирателей. Голосование по доверенности было запрещено, про-

изводилось лично избирателем. Избиратель после голосования опускал палец в несмываемые чернила, чтобы он не мог голосовать дважды. На рис. 2 показан избирательный бюллетень [5].

Рис. 3. Электронное устройство

Подсчет голосов. На выборах 2018 года, IHEC впервые использовала сканирующее устройство для подсчета результатов и передачи результатов с избирательных участков в центры подсчета голосов. Избиратель ставил перед своим кандидатом отметку специальной ручкой, на которую наносили логотип IHEC, чтобы избежать фальсификаций. Далее избиратель вставлял бюллетень в сканирующее устройство. Оно считывало отметку избирателя, сортировало и подсчитывало бюллетени. На рис. 3 изображено электронное устройство, которое использовалось на иракских выборах в 2018 году [5].

Объявление результатов голосования. Заверенные результаты объявлялись после рассмотрения жалоб избирательной судебной коллегией.
Проведенный анализ системы голосования в республике Ирак позволяет сделать следующие выводы и сформулировать перспективное направление развития системы голосования в республике Ирак.

- Использование биометрической регистрации и верификации на выборах 2018 года является одним из важнейших шагов в переходе к онлайн-голосованию.
- Использование электронного устройства на выборах 2018 года, привело к недостаткам: уязвимость к взлому, возможность фальсификации результатов голосования и замедление избирательного процесса.
- Для повышения безопасности системы голосования, предлагается использовать криптографическую гомоморфную схему для хранения и подсчета голосов в зашифрованном виде. Использование шифрования защитит голоса от манипуляции и фальсификации, гарантирует их тайну и анонимность, повысит эффективность контроля и ускорит процесс подсчета голосов.

Список используемых источников

1. Chalabi M. H. E-voting framework for elections in Iraq. Master's thesis. Managament information system. Univesiti kebangsaan Malaysia. Bangi, 2014. 135 C.
2. Ameen Z. Application voting system of web based in Iraq // Iraqi Journal of Science.
3. Tabra Y. M. A proposal for internet voting system in Iraq // International journal of advanced research in computer science and software engineering. 2013.N10. C 47-52.
4. Ali K. J., Stanley M. P. Online voting system for Iraqi federal government (IFG) // International journal of engineering science & advanced technology. 2013.N 3. C.240-242.017. N 1A. C.192-200.

5. International foundation for electoral systems. Middle East and North Africa. Elections in Iraq 2018 Council of Representatives Elections. www.IFES.org. 2018.

*Статья представлена научным руководителем,
доктором технических наук, профессором В. А. Яковлевым.*

**УДК 004.93
ГРНТИ 28.23.15**

МЕТОД РЕШЕНИЯ ЗАДАЧИ КОМПЬЮТЕРНОГО ЗРЕНИЯ ПО ПОИСКУ ПРОСТЫХ ФОРМ НА ИЗОБРАЖЕНИИ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМА ХАФА

С. С. Сергиенко, А. В. Фёдорова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена методу решения задач компьютерного зрения по поиску простых геометрических форм на изображениях. Рассматриваются принципы преобразования Хафа для нахождения прямых линий и окружностей. Показана реализация этого алгоритма путем написания кода на языке программирования Python с использованием библиотеки алгоритмов компьютерного зрения OpenCV. Показано влияние параметров оператора Хафа на обнаружение искомых форм. Продемонстрированы возможности использования данного алгоритма для решения задачи детектирования объектов, ввиду того, что простые геометрические фигуры являются наиболее распространенными формами, встречающимися в окружающей среде.

компьютерное зрение, преобразование Хафа, библиотека OpenCV, поиск геометрических форм.

Технология компьютерного зрения является научным направлением в области искусственного интеллекта для получения изображений объектов реального мира, их обработки и использования полученных данных для решения разного рода прикладных задач без полного или частичного участия человека [1].

Одним из методов компьютерного зрения для поиска объектов, принадлежащих определенному классу фигур, например линий или окружностей, является метод, использующий алгоритм, основанный на преобразовании Хафа. Имеется пространство параметров, в котором происходит процедура голосования, и в соответствии с локальными максимумами определяется наиболее вероятное положение искомой фигуры.

Для поиска линий идея преобразования состоит в том, что прямую на плоскости можно охарактеризовать уравнением:

$$x \cdot \cos\theta + y \cdot \sin\theta = \rho, \quad (1)$$

где (x, y) – декартовы координаты, (ρ, θ) – параметры пространства Хафа.

Данное уравнение соответствует точке с координатами (x, y), через которую проходит прямая. Плоскость (ρ, θ) называют пространством параметров или пространством Хафа, а плоскость (x, y) декартовой плоскостью. Также каждая прямая может быть описана набором точек. Если синусоиды соответствующие двум точкам декартовой плоскости наложить друг на друга, то точка в пространстве Хафа, где они пересекутся, будет соответствовать параметрам прямой, проходящей через обе эти точки [2]. Таким образом, для обнаружения прямых на исходном изображении достаточно найти все значительные локальные максимумы аккумуляторной функции $A(\rho, \theta)$. для каждой точки пространства параметров суммируется количество голосов, поданных за нее, т. е. число точек исходного пространства, порождающих в пространстве параметров отклики, проходящие через данную точку (ρ, θ) [3]. Пример использования алгоритма приведен на рис. 1.

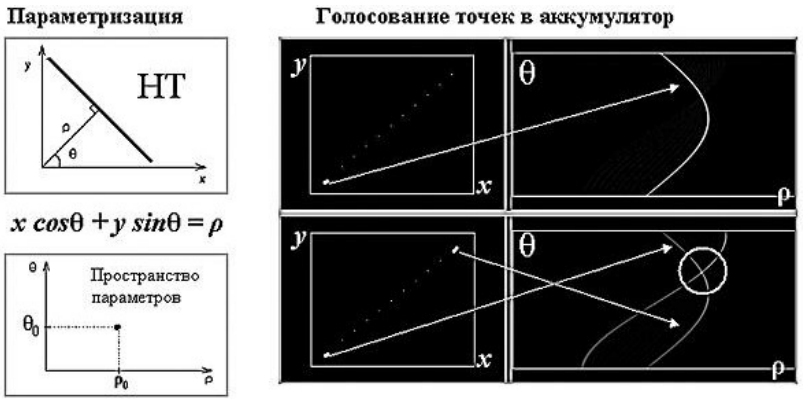


Рис. 1. Пример использования алгоритма Хафа для поиска прямых
Источник: Преобразование Хафа для поиска прямых – Техническое зрение. URL: https://inlnk.ru/rj80J (дата обращения 22.02.21)

Если рассматривать поиск окружностей, то тут уже используется три параметра – координаты центра и радиус. Если известен радиус, задача двумерна. Имея множество точек, можно принять их за возможные центры окружностей радиуса R. Положение наиболее вероятной в конкретном множестве точек окружности соответствует точке пересечения максимального числа голосующих окружностей [2]. Иллюстрация применения алгоритма приведена на рис. 2.

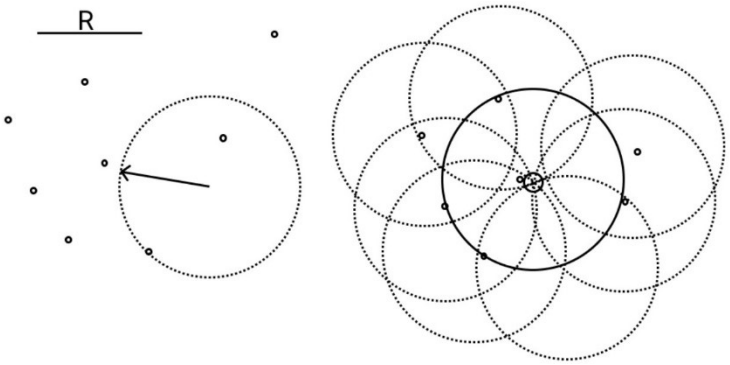


Рис. 2. Иллюстрация преобразования Хафа для поиска окружностей [Преобразование Хафа для поиска окружностей – Техническое зрение. URL: https://inlnk.ru/rYomo (дата обращения: 23.02.21)]

Программная реализация данного алгоритма возможна на языке Python с помощью библиотеки компьютерного зрения OpenCV. В результате эксперимента был написан код, результатом работы которого является выделение синим цветом всех объектов, найденных на изображении со случайным набором линий и окружностей, и зеленым цветом линий и окружностей с максимальными величинами длины или радиуса. Результат программной реализации алгоритма показан на рис. 3.

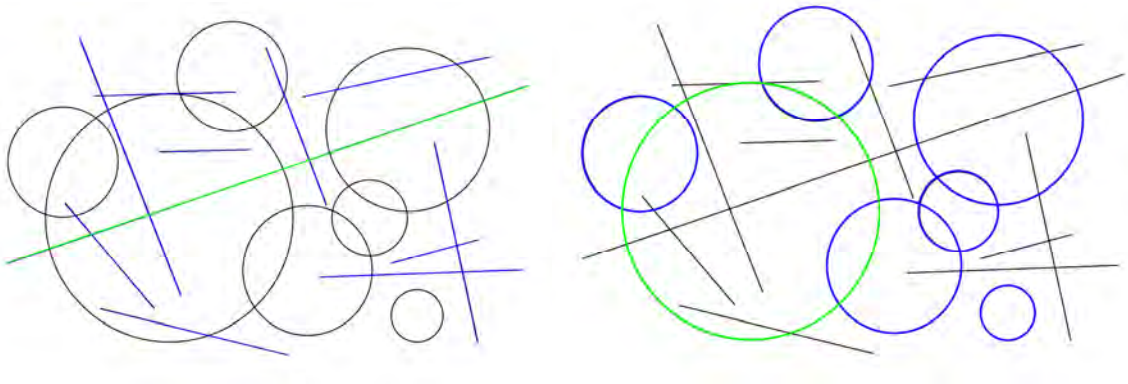


Рис. 3. Результат работы программы по поиску геометрических форм

Поиск линий осуществляется с помощь функции HoughLines, на вход которой поступают изображение, параметры разрешения по дистанции и по углу ρ и θ, пороговый параметр аккумулятора, минимальная длина линии и максимальный разрешенный промежуток между точками на одной линии для их соединения [5]. Для поиска окружностей используется функция HoughCircles, параметры которой верхнее пороговое значение, передаваемое детектору границ, разрешение сумматора, используемое для детектирования центров кругов, минимальная дистанция между центрами детектируемых кругов и два параметра, зависящие от метода трансформации [6]. Результат поиска очень сильно зависит от параметров. Например, при поиске линий при изменении параметра θ найденные линии становятся короче,

чем они есть, а при изменении ρ находятся короткие линии на окружности. Также при поиске окружностей возможно нахождение большого количества лишних окружностей или, наоборот, меньшего, чем есть на исходном изображении.

При работе с цветными изображениями для нахождения линий требуется произвести предварительную обработку. К оригиналу изображения применяется черно-белый фильтр, далее морфологическая очистка от шумов, детектор границ, выделяющий контуры линий и финальным шагом является выделение найденных линий. Описанные этапы показаны на рис. 4.

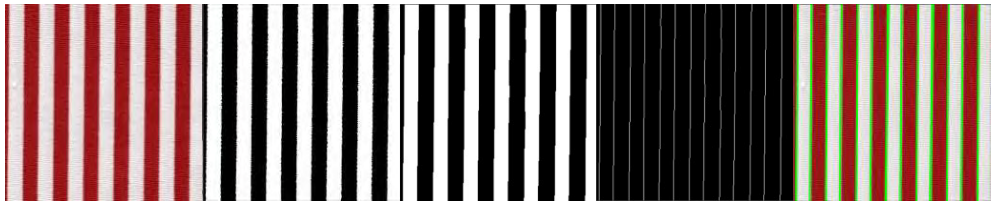


Рис. 4. Этапы обработки цветного изображения для поиска линий на нем

Если применить тот же код к похожему изображению, то возможна его некорректная работа, как в случае с примером, показанным на рис. 5, где красным цветом сначала выделено все изображение, что говорит о нахождении большого количества лишних линий. При изменении параметров алгоритм находит правильные линии.

Рис. 5. Некорректная работа алгоритма
при одинаковых параметрах функции Хафа

Выявление выше описанной чувствительности алгоритма и необходимость ручного подбора параметров может сделать программную реализацию алгоритма неподходящей для применения в реальной жизни. Например, для поиска линий дорожной разметки, где важна высокая точность и скорость, не представляется возможным подбирать параметры вручную в зависимости от качества изображения, освещения дороги и других условий. Пример нахождения линий дорожной разметки представлен на рис. 6.

Рис. 6. Поиск линий дорожной разметки

В данном примере алгоритм применяется к изображению хорошего качества с хорошо выделяемыми линиями. Для другого изображения такой же набор параметров функции Хафа в большинстве случаев будет неподходящим. Но учитывая простоту реализации, хорошее детектирование геометрических объектов при правильной настройке, данный алгоритм имеет место быть при соответствующей доработке.

Преобразование Хафа хорошо зарекомендовало себя для поиска параметрически задаваемых объектов, но в процессе применения этого алгоритма на практике замечена высокая чувствительность алгоритма к задаваемым параметрам, что значительно снижает его эффективность. Таким образом, возникает необходимость предусмотрения возможности автоматизированной настройки параметров.

Список используемых источников

1. Компьютерное зрение – Викиконспекты. URL: https://inlnk.ru/WRJQB (дата обращения 22.02.21)

2. Кудрина М.А. Использование преобразования Хафа для обнаружения прямых линий и окружностей на изображении // Известия Самарского научного центра Российской академии наук. 2014. № 4 (2). С. 476–478.

3. Преобразование Хафа для поиска прямых – Техническое зрение. URL: https://inlnk.ru/rj80J (дата обращения 22.02.21)

4. Преобразование Хафа для поиска окружностей – Техническое зрение. URL: https://inlnk.ru/rYomo (дата обращения 23.02.21)

5. Hough Line Transform – OpenCV-Python Tutorials 1 documentation. URL: https://opencv-python-tutroals.readthedocs.io/ en/latest/py_tutorials/ py_imgproc/py_houghlines/py_houghlines.html (дата обращения 27.02.20)

6. OpenCV шаг за шагом. Преобразование Хафа. URL: http://robocraft.ru/blog/computervision/502.html (дата обращения 01.03.21)

УДК 621.391
ГРНТИ 49.03.03

ОЦЕНКА УСЛОВИЙ ОТКРЫТОГО СЕТЕВОГО МНОГОКЛЮЧЕВОГО СОГЛАСОВАНИЯ

А. Д. Синюк, А. А. Тарасов

Военная академия связи

Одним из основных условий функционирования телекоммуникационных систем, использующих криптографические методы защиты информации, является безопасная установка ключей корреспондентам. Менее затратной альтернативой передаче ключей по защищенным каналам связи выступают методы ключевого согласования по открытым каналам. Актуализируются исследования формирования увеличенной криптосвязности сетевых корреспондентов путем оценки условий осуществления предлагаемого метода открытого сетевого многоключевого согласования.

ключ, информационная скорость, открытое сетевое многоключевое согласование.

Важнейшим направлением обеспечения информационной безопасности телекоммуникационных систем, использующих для защиты информации криптографические методы, является эффективное решение задачи формирования, распределения и доставки ключей корреспондентам. Сложными этапами ее решения являются безопасные формирование, а также распределение и доставка ключей законным корреспондентам с использованием защищенных каналов связи, что достаточно дорого, не всегда оперативно и возможно.

Альтернативой выступают способы формирования ключей посредством передачи информации по каналам связи, которая, возможно, становится известной нарушителю. Ранее стали известны результаты исследований для некоторых способов открытого ключевого согласования двух законных корреспондентов [1, 2, 3, 4]. Несколько позже опубликованы результаты исследований условий открытого формирования сетевого (группового) ключа [5].

Ключевая структура, объединяющая трех и более корреспондентов с общим сетевым ключом в наибольшей степени подвержена разрушению нарушителем, осуществившим компрометацию общего ключа [5]. Закрытый информационный обмен между корреспондентами в подобной телекоммуникационной системе становится невозможным и требует незамедлительного решения задач формирования, распределения и доставки нового сетевого ключа корреспондентам. Уменьшение информационных потерь в закрытой сети связи можно получить за счет уменьшения временных затрат

на восстановление сетевого ключа. Одним из путей решения этой задачи является в дополнение к сформированному сетевому ключу обеспечение корреспондентов сети связи ключами попарной связи. Поэтому, большой практический интерес представляет оценка возможности осуществления открытого сетевого многоключевого согласования. В этих условиях актуализируется постановка задачи согласования некоторого множества ключей по каналам сети связи, подверженным перехвату нарушителем в целях одновременного формирования по открытым каналам связи между корреспондентами сети, как сетевого общего ключа, так и ключей между парами корреспондентов связи.

Рассмотрим следующую постановку задачи передачи информации по широковещательному каналу связи [6, 7, 8], описывающему модель канальной связности сети связи. Имеется один передатчик у корреспондента связи (КС) *A* и три независимо работающих приемника у КС *B*, *C* и нарушителя *E*, на входы которых поступают выходные сигналы разных каналов. На передатчик КС *A* поступают сообщения от источника *G*1, которые он должен передать одновременно приемникам 1, 2 и 3 (КС *B*, *C* и нарушителю *E*) так, чтобы приемники 1 и 2 могли восстановить с произвольно малой вероятностью ошибки сообщения *G*1, а нарушитель не имел этой возможности.

Сделаем ряд предположений. Пусть источник сообщений *G*1 описывается моделью двоичного источника без памяти [6]. Алфавит источника задается ансамблем $\{G, p(g)\}$, где G – множество состоящее из $t = 2$ букв $G = \{0,1\}$. Источник в каждую единицу времени независимо выбирает *i*-ю букву из алфавита некоторой вероятностью $p(g_i)$. Пусть задано достаточно большое *n*. Источник генерирует сообщение $\bar{g}$, представляющее собой последовательность длиной *n* букв источника, причем $\bar{g} \in G^n$, где G^n – *n*-я декартова степень множества *G*. Совокупность, состоящая из двух каналов с общим входом (выход источника *G*1) и выходами (входы приемников 1, 2) описывается моделью дискретного широковещательного канала без памяти (ДШКБП) [6].

Передача сигналов по ДШКБП определяется двумя составляющими каналами с общим входным алфавитом *G,* выходными алфавитами *Y* (для первого составляющего канала связи) и *M* (второй составляющий канал) и матрицами переходных вероятностей $P_1 = \{p(y/g)\}, P_2 = \{p(m/g)\}, g \in G,$ $y \in Y, m \in M$. Алфавиты *G, Y* и *M* конечны и для любых последовательностей $\bar{g} \in G^n, \bar{y} \in Y^n, \bar{m} \in M^n$, где G^n, Y^n, M^n – декартовые *n*-е степени множеств *G*, *Y*, *M*, соответственно. Сделаем предположение, что первый составляющий канал связи, описывается моделью двоичного симметричного канала связи без памяти (ДСКБП) с вероятностью ошибки p_y, а второй – моделью ДСКБП с вероятностью ошибки p_m. Канал связи между выходом источника КС *A* и входом приемника 3 нарушителя *E* представляет собой

канал перехвата (КП) нарушителя. Передача сигналов по КП определяется входным конечным алфавитом *G,* выходным алфавитом *Z* и матрицей переходных вероятностей $P_3 = \{p(z/g)\}, g \in G, z \in Z$. Канал перехвата описывается моделью ДСКБП с вероятностью ошибки p_w. Предположим, что составляющие ДШКБП и КП являются независимыми каналами [6, 7]. Алфавиты источника *G*1, входа и выхода ДШКБП и КП, совпадают. В целях некоторого упрощения исследования исключим из рассмотрения нарушителя *E* и сделаем предположение, что КП находится в состоянии «обрыва» [6, 7], т. е. $p_w = 0{,}5$.

Произведем оценку ситуации после передачи $\overline{g}$ от КС *A* по ДШКБП последовательности $\overline{g}$ КС *B* и *C* принимают свои версии $\overline{y} \in Y^n$ и $\overline{m} \in M^n$, соответственно. Оценим информационную скорость каждого из каналов по отдельности: ДШКБП, первого составляющего канала (СК1) и второго составляющего канала (СК2). В заданных условиях скорость ДШКБП [бит/симв] может быть определена из выражения:

$$V_{\text{ДШКБП}} = \frac{F\left(G^n; Y^n; M^n\right)}{n} = F\left(G; Y; M\right), \tag{1}$$

где $F\left(G; Y; M\right)$ – средняя совместная информация между соответствующими символами на входе и выходе ДШКБП [9]. Подобным образом можно найти информационную скорость СК1 и СК2 [бит/симв]:

$$V_{\text{СК1}} = \frac{I\left(G^n; Y^n\right)}{n} = I\left(G; Y\right), \tag{2}$$

где $I\left(G; Y\right)$ – средняя взаимная информация между соответствующими символами на входе и выходе СК1 [6, 7] и

$$V_{\text{СК2}} = \frac{I\left(G^n; M^n\right)}{n} = I\left(G; M\right), \tag{3}$$

где $I\left(G; M\right)$ – взаимная информация СК2.

Пусть вероятности ошибок в СК1 и СК2 удовлетворяют неравенству:

$$0 < p_y \le p_m < 0{,}5. \tag{4}$$

Тогда в соответствии с (1)–(4) значения информационных скоростей каналов будут располагаться по возрастанию в соответствии с неравенством:

$$V_{\text{ДШКБП}} < V_{\text{СК2}} \le V_{\text{СК1}}. \quad (5)$$

Предположим, что для получения информационной основы формируемого ключа достаточно передать по каналу связи количество информации равное S бит, причем выполняется условие:

$$S = nV_{\text{ДШКБП}}. \quad (6)$$

Для СК1 и СК2 из (6) и с учетом (2) и (3) могут быть найдены числа символов $n1$ и $n2$ необходимых для формирования ключа в соответствующих каналах:

$$n1 = \frac{S}{V_{\text{СК1}}},\ n2 = \frac{S}{V_{\text{СК2}}}. \quad (7)$$

Заметим, что числа n, $n1$, $n2$ в общем случае не равны и в соответствии с (1)–(7) удовлетворяют неравенству:

$$n1 \le n2 < n. \quad (8)$$

Анализ (8) показывает, что если для формирования информационной основы сетевого ключа необходимо передать по ДШКБП последовательность $\overline{g}$ (и принять на его выходах $\overline{y}$ и $\overline{m}$) длиной n символов, то для формирования информационной основы парного ключа между КС A и C можно использовать из $\overline{g}$ и $\overline{m}$ меньшее число $n2$ соответствующих символов, а для формирования основы ключа между КС A и B можно использовать из $\overline{g}$ и $\overline{y}$ еще меньшее число $n1$ символов. Это определяет предварительные условия формирования различных двух парных и одного сетевого ключей. Даже при условии, когда $n1 = n2$ и высокой вероятности формирования в СК1 и СК2 различных «векторов ошибок» [6, 7] сохраняется возможность формирования различных парных ключей.

Подводя итог, отметим, что в работе рассмотрены теоретико-информационные условия открытого сетевого многоключевого согласования. Остались не освещенными ряд вопросов, которые могут выступить в роли направлений дальнейших исследований связанных с обобщением на модели других источников и широковещательных каналов, введением нарушителя, оценкой информационной эффективности, синтезом протоколов открытого сетевого многоключевого согласования, применением ключей и др.

Список используемых источников

1. Csisar, I.; Korner, J. Broadcast channels with confidential messages // IEEE Trans. On IT. vol. 24. no. 3. 1978. Pp. 339–348.
2. Wyner, A. The wire–tap channel // Bell Syst. Techn. J. vol. 54. no 8. 1975, Pp. 1355–1387.
3. Maurer, U. Secret Key Agreement by Public Discussion Based on Common Information // IEEE Trans. on IT. Vol. 39, May 1993. Pp. 733–742.
4. Яковлев В., Коржик В., Бакаев М. Протоколы формирования ключа на основе каналов связи с шумом в условиях активного перехвата с использованием экстракторов // Проблемы информационной безопасности. Компьютерные системы. № 1. СПб.: СПбГТУ, 2006. С. 60–81.
5. Синюк А. Д. Формирование трехстороннего шифрключа по открытым каналам связи с ошибками. Монография. СПб.: ВАС, 2009. 360 с.
6. Колесник В. Д., Полтырев Г. Ш. Курс теории информации. М.: Наука. Главная редакция физико-математической литературы, 1982. 416 с.
7. Чисар И., Кернер Я. Теория информации: теоремы кодирования для дискретных систем без памяти: Пер. с англ. М.: Мир, 1985. 400 с.
8. Cover T. Broadcast Channels. IEEE Trans, on Inf. Theory, 1972, vol. 18, № 1.
9. Остроумов О. А., Синюк А. Д. Исследование совместной информации // Информация и космос. 2017. № 3. С. 55–58.

УДК 004.382.72
ГРНТИ 50.33.35

КОНЦЕПЦИЯ МОБИЛЬНОГО ЛАБОРАТОРНОГО КОМПЛЕКСА ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В. А. Тарасов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Новые технологические решения в области электроники и вычислительной техники открывают дополнительные возможности для реализации образовательного процесса. Рассмотрена проблематика, связанная с особенностями лабораторно-технической базы, использующейся для изучения информационных технологий. Проведён краткий обзор аппаратных платформ. Приведены варианты их использования. Предложен вариант лабораторного комплекса, отражены его преимущества.

Raspberry Pi, одноплатный компьютер, образовательный процесс, лабораторный комплекс, информационные технологии.

Практическое освоение информационных технологий для современного человека является важным аспектом жизни, особенно, если его сфера деятельности и профиль подготовки непосредственно связаны с автоматизацией информационных процессов. В области образования, в том числе в высшей школе, зачастую организационные и лабораторно-технические особенности образовательного процесса не всегда позволяют гибко адаптировать аппаратно-программную платформу.

Особенно это заметно в сфере освоения динамично развивающихся информационных технологий. Новые программные средства требуют более производительных платформ, чем предыдущие. А порой может возникнуть потребность в изменении конфигурации лабораторной информационной системы.

Для проведения лабораторных занятий, связанных с формированием компетенций в области информационных технологий, а точнее – освоением современных базовых, системных, служебных и прикладных программных средств, используются лаборатории, оснащённые, как правило, стационарными лабораторными компьютерами, используемыми студентами и преподавателями в качестве универсальных инструментов для изучения различных продуктов. В этой связи можно выделить следующие сложности.

Во-первых, можно столкнуться с недостаточной производительностью оборудования и необходимостью хранить на носителях множество различной информации, интенсивным использованием оборудования, что в комплексе, при использовании накопителей на жёстких магнитных дисках, приводит со временем к уменьшению скорости доступа к данным.

Во-вторых, применение технологий виртуализации ограничивает возможности, а в некоторых случаях (например, при необходимости доступа к BIOS) делает невозможным изучение некоторых вопросов. Кроме того, использование виртуальных машин способно существенно замедлить работу, а некоторые продукты требуют особой их настройки либо вообще не функционируют на них корректно.

В-третьих, в условиях множественности учебных дисциплин используется общая политика безопасности. Для большинства предметных областей это приемлемо. Но полноценное обучение информационным технологиям требует гибкой информационной инфраструктуры. Иными словами, у обучающихся может возникнуть необходимость в самостоятельной установке программных продуктов и их компонентов, а также в иных операциях, связанных с доступом к системным ресурсам, что в условиях применения стандартных политик безопасности (иначе говоря, запретов изменений в системе) не даёт реализовать некоторые задачи.

Несколько лет назад было анонсировано начало продаж одноплатных компьютеров под маркой Raspberry Pi (рис.). Данная платформа стала основой целого семейства и примером для ряда альтернативных разработок [1].

Недавно представленная новая версия мини компьютера Raspberry Pi 4 обладает значительной производительностью – четырехъядерный 64-битный процессор с тактовой частотой 1,5 ГГц, два порта USB 2.0 и два USB 3.0, Bluetooth 5.0, поддержка двух мониторов, GPU VideoCore VI способен обработать видеопоток формата 4K с 60 fps, есть возможность выбора объема ОЗУ – 1, 2 или 4 Гбайт LPDDR4 SDRAM.

Аналогами данного продукта являются Orange Pi Prime, Banana Pi M3, Rock64, ASUS Tinker board S, Libre Computer Renegade и Renegade Elite, Odroid H2, Arduino Mega 2560 и др. Некоторые характеристики этих устройств представлены в таблице.

Следует отметить, что Raspberry Pi поддерживает операционные системы преимущественно семейства Linux. Однако, скорее всего, с ростом популярности и расширением областей применения платформы, увеличением её производительности и функционала перечень поддерживаемых систем будет расширяться.

Одноплатные платформы широко используются для решения различных задач, в числе которых управление технологическими процессами, аудит информационной безопасности, формирование лабораторного базиса для учебных целей.

Они могут быть успешно применены для изучения вопросов администрирования информационных систем.

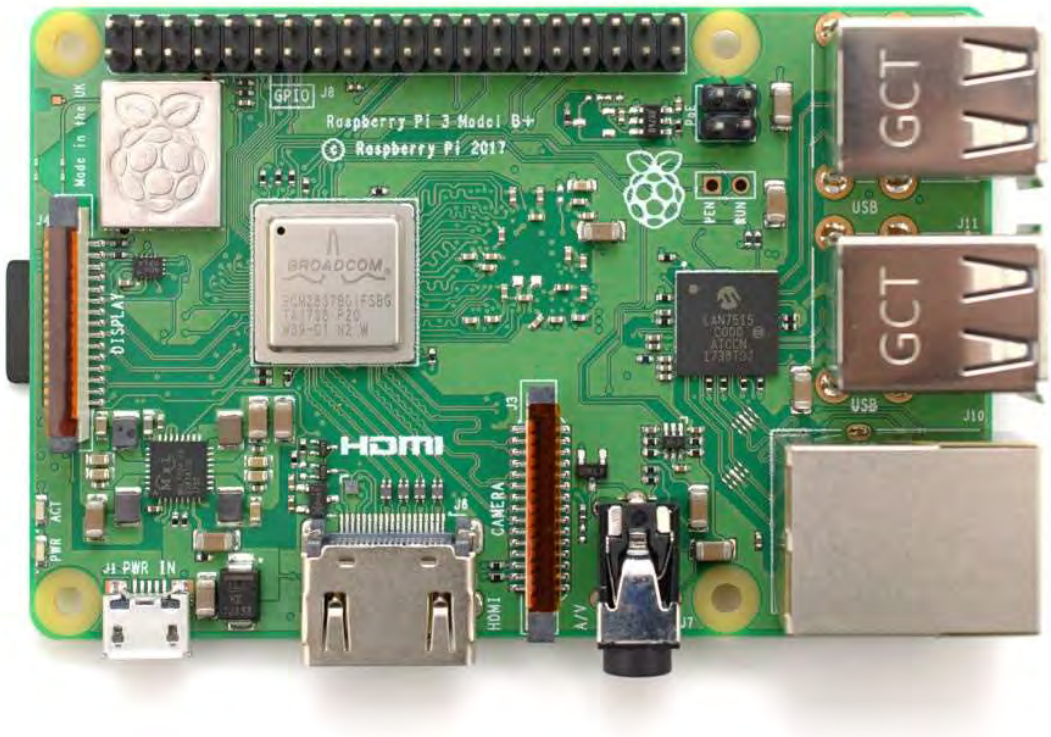


Рис. Платформа Raspberry Pi

В частности, на платформе Raspberry Pi 2 предложена клиент-серверная информационно-управляющая система дистанционного обучения, призванная решать задачи управления обучением, управления взаимодействием участников образовательного процесса посредством чата, видеоконференций, виртуальных комнат, технической и методической поддержки слушателей в виде тестирования, видеоуроков. В качестве сервера предлагаются варианты аренды выделенного сервера либо хостинга [2].

Иной вариант использования в обучении – Raspberry Pi 3 для проведения занятий, требующих наличия специального программного обеспечения и средств разработки. В данном случае для организации вычислений предлагается использовать облачные технологии. Декларируется работа на базе микрокомпьютеров без потери функциональности и производительности и внедрение кластера с вычислительной мощностью в виде 24-потокового процессора и 144 Гб оперативной памяти, а также возможность параллельной работы с высокой производительностью в облаке не менее чем 40 рабочих мест, что эквивалентно полноценной учебной лаборатории [3].

В свете вышеизложенного представляется целесообразным формирование для решения специализированных задач мобильных лабораторных комплексов на базе микрокомпьютеров. Данное оборудование может быть оперативно размещено на любых площадях.

ТАБЛИЦА. Характеристики одноплатных платформ

Модель	ОЗУ	Флэш	USB	Ethernet	Wi-Fi
Raspberry Pi 3B+	1 Гбайт	Слот MicroSDHC	4	1 000 Мбит/с	802.11 b/g/n/ac 2.4/5 ГГц
Raspberry Pi Zero	512 Мбайт	Слот MicroSDHC	1	-	-
Raspberry Pi Zero W	512 Мбайт	Слот MicroSDHC	1	-	802.11 b/g/n
Banana Pi M3	2 Гбайт LPDDR3	8 Гбайт eMMC	3 (2 × 2.0, 1 × OTG)	1 000 Мбит/с	802.11 b/g/n
Banana Pi M2 Zero	512 Мбайт DDR3	Слот MicroSDHC	1 × USB 2.0 OTG	-	802.11 n
Rock64	4 Гбайт LPDDR3	128 Мбайт	3 (3.0, 2.0, OTG)	1 000 Мбит/с	802.11 b/g/n
Asus Tinker board S	2 Гбайт LPDDR3	16 Гбайт eMMC	4 × USB 2.0	1000 Мбит/с	802.11 b/g/n
Libre Computer Renegade	4 Гбайт DDR4	-	3 (1 × 3.0, 1 × 2.0)	1 000 Мбит/с	-

Модель	ОЗУ	Флэш	USB	Ethernet	Wi-Fi
Libre Computer Renegade Elite	4 Гбайт DDR4	128 Мбайт	5 (2 × 3.0, 3 × 2.0)	1 000 Мбит/с	-
Odroid H2	2 слота DDR4 SO-DIMM	128 Мбайт (BIOS), слот eMMC	4 (2 × 3.0, 2 × 2.0)	2 × 1 000 Мбит/с	-
Arduino Mega	8 кбайт	256 кбайт	USB-UART преобразователь	-	-

Группа одноплатных компьютеров в специализированных корпусах с портативными мониторами, объединённых коммутатором, в ряде случаев способна заменить стационарную лабораторную базу с настольными компьютерами, но имеет перед последней ряд преимуществ.

1. Стоимость. Данный комплекс намного дешевле обычного лабораторного при сопоставимой производительности.

2. Компактность. Весь комплекс можно уместить в одном-двух обычных кейсах, масса его весьма невелика. Следствие – возможность быстрого развёртывания и свёртывания.

3. Мобильность. Оборудование может быть размещено в любом помещении, а при наличии автономного питания – вне его.

4. Малое энергопотребление. Данное обстоятельство не очень существенно, однако является преимуществом.

5. Возможность распределённой работы. При подключении к системе беспроводного доступа либо иной сетевой инфраструктуре элементы комплекса могут взаимодействовать на значительном удалении.

6. Широкие возможности использования. Компоненты рассматриваемой системы могут использоваться для локальной работы в качестве лабораторного компьютера, в рамках совместной работы в сети, для создания кластера, в качестве компонентов робототехнических комплексов как звено управления и т. д.

7. Гибкость конфигурации. Пожалуй, главное преимущество комплекса. Независимость от политики информационной безопасности и возможность установки необходимого состава программного обеспечения (в пределах ресурсов платформы) дают возможность обучающимся самостоятельно формировать конфигурацию и осуществлять администрирование информационной системы.

Отдельного внимания заслуживает вопрос подключения выделенного сервера, весьма важного компонента в рамках системного администрирования. Выделенный сервер должен отличаться повышенной надёжностью и производительностью по сравнению с рабочими станциями. В этой связи

в качестве такового можно использовать стационарную ЭВМ или даже ноутбук, решение следует принимать в зависимости от задачи и возможностей.

Таким образом, возможны альтернативные варианты реализации лабораторных комплексов, способные решать широкий круг задач.

Список используемых источников

1. Альтернативы Raspberry Pi // Хабр. URL: https://habr.com/ru/post/457666/ (дата обращения 03.04.2020).

2. Мазуров Д. Н. Исследование и разработка клиент-серверной информационно-управляющей системы дистанционного обучения на базе микрокомпьютера Raspberry Pi 2 // Всероссийская научная конференция по проблемам управления в технических системах : материалы науч. конф., Санкт-Петербург, 28-30 окт. 2015 г. СПб : СПбГЭТУ «ЛЭТИ», 2015. № 1. С. 377–379.

3. Кузьмичев А. Б. Оптимизация образовательного процесса при проведении практических занятий по направлениям обучения, требующих наличия специального прикладного программного обеспечения и средств разработки программного обеспечения // Балтийский гуманитарный журнал. 2017. Т. 6. N 4 (21). С. 323–326.

Статья представлена заведующим кафедрой ИУС СПбГУТ, доктором технических наук, профессором Л. К. Птицыной.

УДК 37.025.7
ГРНТИ 14.37.01

ИНФОРМАЦИОННАЯ СИСТЕМА ДЛЯ РАЗВИТИЯ КОГНИТИВНЫХ СПОСОБНОСТЕЙ

В. А. Тарасов, Е. М. Чернобровкин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Развитие когнитивных функций мозга происходит, по большей части, в детстве. Потребность в дальнейшем развитии может проявить себя гораздо позже – например, в школе в виде плохой успеваемости (затрудненное запоминание, неспособность сосредоточиться, высокая утомляемость). Логичным представляется уделить больше времени проблемным фрагментам деятельности, однако данный подход редко находит отклик, так как он трудоемок и непривлекателен. На сегодняшний день существует немало программных сервисов, предлагающих разного рода улучшение работы мозга в целом. Это могут быть всевозможные пазлы или тренажеры памяти. Рассматриваются вопросы эффективности применения информационных технологий для развития когнитивных способностей.

когнитивные способности, логическое мышление, способ обучения, системы развития, образовательные информационные технологии.

Когнитивное развитие – развитие всех видов мыслительных процессов, таких как восприятие, память, формирование понятий, решение задач, воображение и логика.

Недостаточная степень развития когнитивных навыков может замедлять или даже препятствовать мыслительной деятельности. Чаще всего подобные проблемы бывают замечены в среде, когда результат мыслительной деятельности заранее известен и вопрос стоит лишь в скорости выполнения задания – школа, университет, потоковая рабочая среда.

В школьной среде для работы с отстающими введена должность школьного психолога, на которого ложится задача тренировки нужных навыков, однако после школы развитие людей становится предоставлено им самим.

Известны следующие механизмы развития когнитивных способностей.

Психологический подход представляет значительное количество программ по диагностике и развитию когнитивных функций, произвольности поведения, эмоционально-волевой сферы дошкольника [1]. Это, безусловно, очень эффективные программы, однако рассчитаны они на дошкольников и младших школьников. А существующие психологические программы по развитию когнитивных функций для взрослых (студентов, профессионалов) и старшеклассников, к сожалению, обладают рядом недостатков, главный из которых – отсутствие экспериментального подтверждения эффективности предлагаемых методик [2].

Педагогический способ начинается с подготовкой к школе, когда внешние обстоятельства (педагог, родитель) в явной форме ставят перед учеником задачу по освоению конкретного материала с предоставленным методом освоения. В основном данный способ практикуется в группах, что уменьшает его эффективность на каждом конкретном обучающемся. За счет большой длительности и постепенного усложнения материала данный подход дает видимый и измеримый результат. Примеры результата – объем выученного стихотворения, сложность используемых абстракций, время концентрации на задаче.

Физический способ подразумевает систематические занятия спортом, особенно игровыми видами [3]. По мнению учёных, в случае малоактивного образа жизни, привычного для современного общества, мозг приспосабливается и снижает когнитивные способности, подчиняясь наиболее энергоэффективной стратегии. Однако, согласно приведенному исследованию, физический способ не может являться полноценным тренингом, а скорее будет полезным дополнением к основной системе развития.

Тренажеры для ума представляют собой широкий спектр логических игр или головоломок, зачастую предлагаемых в форме коммерческих приложений. Их создатели утверждают, что при помощи подобных игр можно

улучшить работу мозга. Исследования реальной эффективности коммерческих приложений для тренировки умственных способностей ранее проводились неоднократно, но определенных результатов достигнуто не было: отмечалось как улучшение когнитивных функций вследствие использования этих приложений, так и отсутствие какого-либо эффекта от тренировок. Однако крупное исследование [4] не подтвердило итоговую эффективность данных тренажеров. При этом несколько последующих исследований допускали возможность небольшого кратковременного эффекта, не превышающего 4% [5], и сравнивали с эффектом от обычных видеоигр [6].

Первый крупный штраф за «вводящую в заблуждение рекламу» коммерческое приложение с играми-тренажерами получило в 2016 году. На сегодняшний день на веб-сайтах таких приложений можно наблюдать многочисленные исследования, доказывающие эффективность их приложений (рис.). Однако подавляющее большинство исследований, которые предоставляются самими приложениями, проводилось на пожилых людях или людях с отклонениями в развитии [7].

Рис. Фрагмент списка исследований,
предоставляющихся приложением CogniFit

Тренажеры конкретного навыка – узконаправленная разновидность тренажеров для ума. Отличие состоит в том, что в каждое упражнение задействует только один аспект когнитивной деятельности, например, память. Идея таких тренажеров состоит в том, что при тренировке самой часто ис-

пользуемой когнитивной функции, кратковременной памяти, положительный эффект проявится и в других сферах. Первые исследования показывали эффективность данного подхода, однако исследование [8], проведенное более крупной командой под более строгим контролем, опровергло результативность данного подхода.

Задачи «шахматного» типа также можно выделить в отдельный пункт, они включают в себя ситуационные вопросы по интеллектуальным играм с полной информацией. Аналогом шахмат в данном случае могут выступить любые игры шахматного типа, например, го или сёги. Отличие от общих тренажеров заключается в том, что среда тренировки фактически является также местом применения тренируемых навыков. Таким образом, подход к решению конкретных изолированных проблем может быть напрямую реализован в партии с помощью абстрагирования. И действительно, кратковременный положительный эффект найден в рамках исследования [9].

Таким образом, система развития когнитивных способностей в рамках информационной системы обладает ограниченными вариантами содержания. Если перед разрабатываемой системой стоит условие использования только методов с доказанной эффективностью, то разумно было бы реализовать систему с педагогическим подходом, например, систему удаленного получения образования или курсов повышения квалификации.

Альтернативный вариант – система, предлагающая «шахматные» задачи и обладающая средой для использования тренируемых навыков, то есть самой игрой.

В качестве содержимого системы развития когнитивных способностей могут быть представлены тренажеры, которые не влияют на когнитивные способности непосредственно, но создают среду для более эффективного использования уже имеющихся навыков. Примером таких тренажеров могут быть упражнения для развития навыков скорочтения, планирования или анализа информации.

Список используемых источников

1. Гуткина Н. И. Психологическая готовность к школе. М.: Академический Проект, 2004, 184 с.

2. Цукарь А. Я. Развитие пространственного воображения. М.: Водолей, 2000. 144 с.

3. Sleiman, Sama F.; Henry, Jeffrey; Al-Haddad, Rami; El Hayek, Lauretta; Abou Haidar, Edwina; Stringer, Thomas; Ulja, Devyani; Karuppagounder, Saravanan S.; Holson, Edward B.; Ratan, Rajiv R.; Ninan, Ipe. Moses V Chao Exercise promotes the expression of brain derived neurotrophic factor (BDNF) through the action of the ketone body β-hydroxybutyrate, Jun 2, 2016, eLife 2016;5:e15092.

4. Simons, Daniel J Do «Brain-Training» Programs Work? Psychol Sci Public Interest. 2016 Oct.

5. Kable, Joseph W.; Caulfield, M. Kathleen; Falcone, Mary; McConnell, Mairead; Bernardo, Leah; Parthasarathi, Trishala; Cooper, Nicole; Ashare, Rebecca; Audrain-McGovern,

Janet; Hornik, Robert; Diefenbach, Paul; Lee, Frank J. and Lerman, Caryn. No Effect of Commercial Cognitive Training on Brain Activity, Choice Behavior, or Cognitive Performance, Journal of Neuroscience 2 August 2017.

6. AnnDeSmet, SofieCompernolle, TomBaranowski, DebbeThompson, GeertCrombez, KarolienPoels, WendyVan, Lippevelde, SaraBastiaensens, KatrienVan, Cleemput, HeidiVandebosch, IlseDe Bourdeaudhuij A meta-analysis of serious digital games for healthy lifestyle promotion, Preventive Medicine, December 2014, Pages 95-107.

7. CogniFit // URL: https://www.cognifit.com/ru/neuroscience (дата обращения 30.03.2021).

8. A compendium of DNB, WM, IQ information up to 2015 Dual N-Back FAQ, 2009-03-25.

9. Sala, Giovanni, Foley, John P. and Gobet, Fernand The Effects of Chess Instruction on Pupils' Cognitive and Academic Skills: State of the Art and Theoretical Challenges, Front. Psychol., 23 February 2017.

Статья представлена заведующим кафедрой ИУС СПбГУТ, доктором технических наук, профессором Л. К. Птицыной.

УДК 001.89
ГРНТИ 12.41.51

ПРОБЛЕМНЫЕ ВОПРОСЫ О НАУКОМЕТРИЧЕСКИХ ПОКАЗАТЕЛЯХ АВТОРОВ НАУЧНЫХ РАБОТ: ПРИЧИННО-СЛЕДСТВЕННЫЙ АНАЛИЗ

И. М. Татарникова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются вопросы, связанные с получением достоверной информации, характеризующей публикационную активность ученых, качество научной работы. Влияние научного исследования на конкретную область знания и на науки в целом индицируется импакт-фактором. Этот и другие показатели были выработаны специалистами в сфере наукометрии. Проводится причинно-следственный анализ проблем, связанных с изучением и измерением качества научных исследований, искажением в ряде случаев данных в результате использования некорректных критериев. Подчеркивается необходимость критического осмысления отдельных аспектов формирования и использования систем индексирования журналов и рейтингов для оценки научной продуктивности.

наукометрия, импакт-фактор, h-индекс, публикационная активность, цитирование.

Введение

Научная деятельность всегда направлена на получение новых знаний, создание и внедрение технологий, позволяющих повысить качество жизни. Производство новых знаний основывается на бесчисленных часах работы в лабораториях и библиотеках, а также формальных и неформальных взаимодействиях с другими учеными. Изучение и измерение качества научных исследований считается одной из актуальных научных задач современности.

Интерес к количественным показателям научной деятельности вызван прогрессом в области информационно-коммуникационных технологий. Здесь большое влияние оказало повсеместное распространение электронных информационных ресурсов, проникновение Интернета в повседневную жизнь каждого человека и внедрение принципа открытого доступа к научным публикациям. Наукометрия и другие, тесно связанные с ней, дисциплины (библиометрия, киберметрия, вебометрика) активно применяются в научной политике и управлении финансированием науки.

Достоверность и искажение оценки научной продуктивности

Основной индекс качества в системе оценки научной деятельности – подсчет журнальных статей и их цитирований. [1]. Данные цитирования позволяют ранжировать журналы, статьи, исследователей. Помимо цитирования статьи, предметом измерения и оценки стало место публикации (журнал), т. е. импакт-фактор журнала используют для сравнения отдельных научных работ или оценки научно-исследовательской деятельности человека. При анализе списка публикаций отдельного исследователя часто выводится заключение: «она публикуется в хороших журналах» или «большая часть его работ опубликована в журналах низкого уровня» [2]. Действительно, качество журналов может демонстрировать уровень научного исследования, рейтинг отдельного ученого. Но это лишь один из многочисленных индикаторов, и тенденция наделять каждую статью характеристиками журнала, в котором она была опубликована, вызывает сомнение. Предполагается, что статьи в высокорейтинговых журналах лучше цитируются. В то же время анализ цитирования публикаций в журнале «Успехи математических наук», который по данным БД РИНЦ в 2019 г. занял первое место по тематике «Математика», показал, что почти половина опубликованных в нем статей не цитируются (рис. 1). При этом имеются и высокоцитируемые статьи. Например, четыре статьи цитируются более 100 раз (в график не попали, так как их доля составляет менее 1 %).

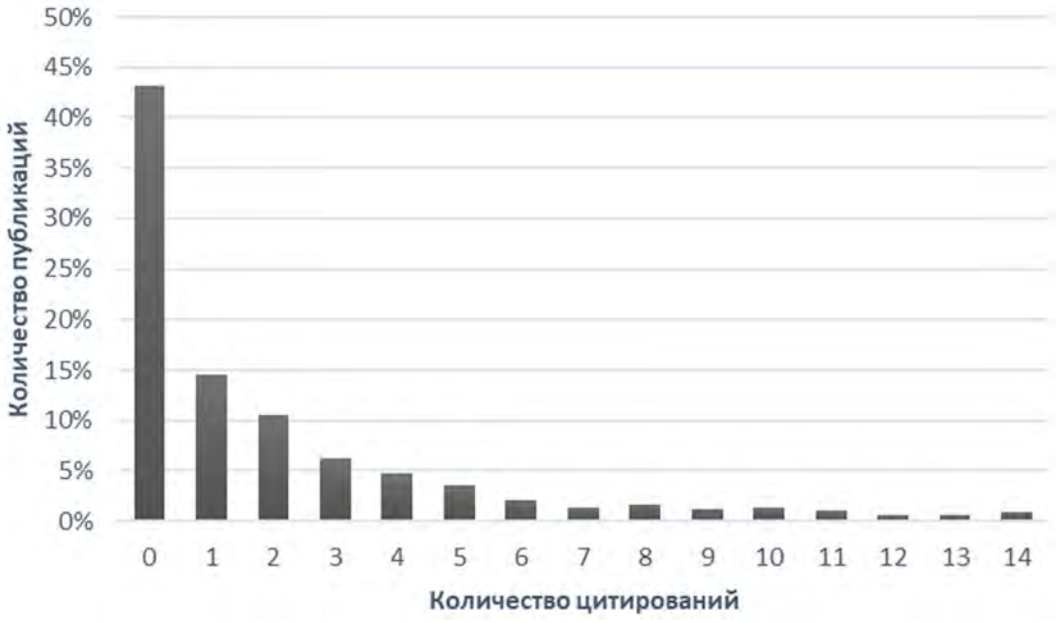


Рис. 1. Распределение публикаций по числу цитирований

Хотя и неверно было бы утверждать, что импакт-фактор совсем ничего не говорит об отдельных статьях в журнале, он дает весьма расплывчатую информацию и может ввести в заблуждение.

Общество ожидает от исследователей публикаций, требующие большого труда, прорывных работ высшего качества. Однако на практике в системе научной коммуникации наблюдаются тенденция к росту в геометрической прогрессии публикационной активности (рис. 2), но в ущерб качеству. Авторы ощущают давление со стороны руководства: установлены границы, за которые публикационная активность падать не может. Редакторам журналов требуется справиться с растущим потоком рукописей и выбрать те, что принесут ссылки за два года. Цитирования вне публикационного окна 2-летнего импакт-фактора (т. е. не в 2-летний период после года выхода в свет) будут бесполезны для рейтинга журнала. Рецензенты вынуждены формально подходить к экспертизе: поток направленных на рецензирование рукописей возрастает, а рецензент в системе научной коммуникации часто совмещает роли всех участников редакционно-издательского процесса: может выступать в качестве автора и редактора. Читатель в свою очередь оказывается не в состоянии прочесть такое количество публикаций [3]. Работы, на которые ссылаются, порой только просматривают.

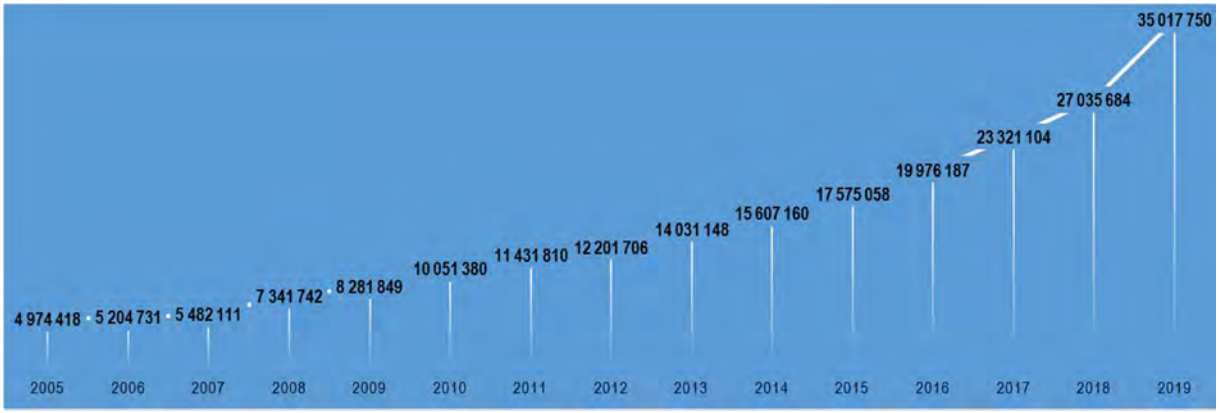


Рис. 2. Динамика роста количества публикаций в БД РИНЦ

В следствии гонки за публикациями и библиографическими индексами мы получаем перепроизводство текстов, публикуемых, чтобы их «посчитали». Статьи выходят с ошибками. Наблюдается кризис экспертной оценки, так как трудно остаться экспертом в традиционном смысле, если по определенному направлению публикуется больше тысячи работ в год, количество научных работников и численность административно-вспомогательного персонала, задействованного в научно-исследовательской работе непрерывно возрастает (рис. 3).

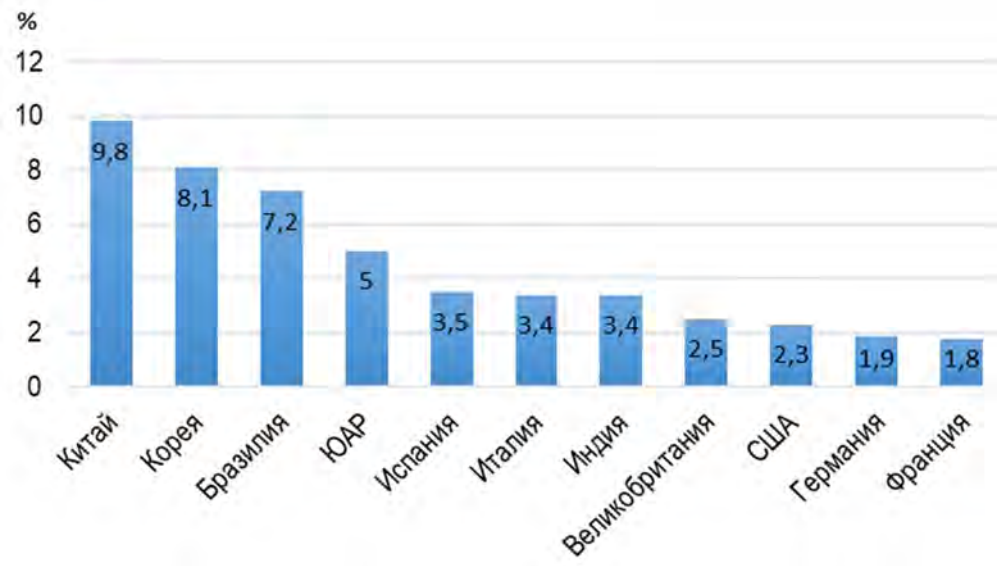


Рис. 3. Среднегодовой темп прироста численности персонала, занятого исследованиями и разработками: 2000–2016 гг. [4]

Физик Хорхе Хирш предложил научному сообществу h-индекс как способ сравнения научных достижений исследователей. В поддержку своего утверждения Хирш приводит данные анализа h-индекса для выборки, состоящей из лауреатов Нобелевской премии [6, 7, 8], индекса Хирш у которых,

как правило, высок. Однако высокий h-индекс сам по себе (без дополнительной информации) вряд ли может дать прогноз по нобелевским лауреатам. Ж. И. Алферов был награжден Нобелевской премией по физике в 2000 г. На начало 2021 г. его индекс Хирша равен 59. В рейтинге БД РИНЦ по своему тематическому направлению он занимает 478-е место, т. е. есть 477 исследователей, которые имеют h-индекс выше, чем у него (можно ли считать их потенциальными лауреатами Нобелевской премии?).

Современные исследователи все чаще приходят к мысли, что этот показатель не измеряет ни количество, ни качество, а представляет собой сочетание этих двух параметров [2, 8, 9, 10]. Методика расчета Хирша учитывает лишь качество, «подкрепленное» количеством, при этом игнорируется «лишнее» качество и количество. А значит, индекс Хирша более всего выгоден для авторов, которые умело вписались в систему создания работ и обмена ссылками с группой исследователей, отвечающих им тем же, и не претендующих на мировое признание (рис. 4).

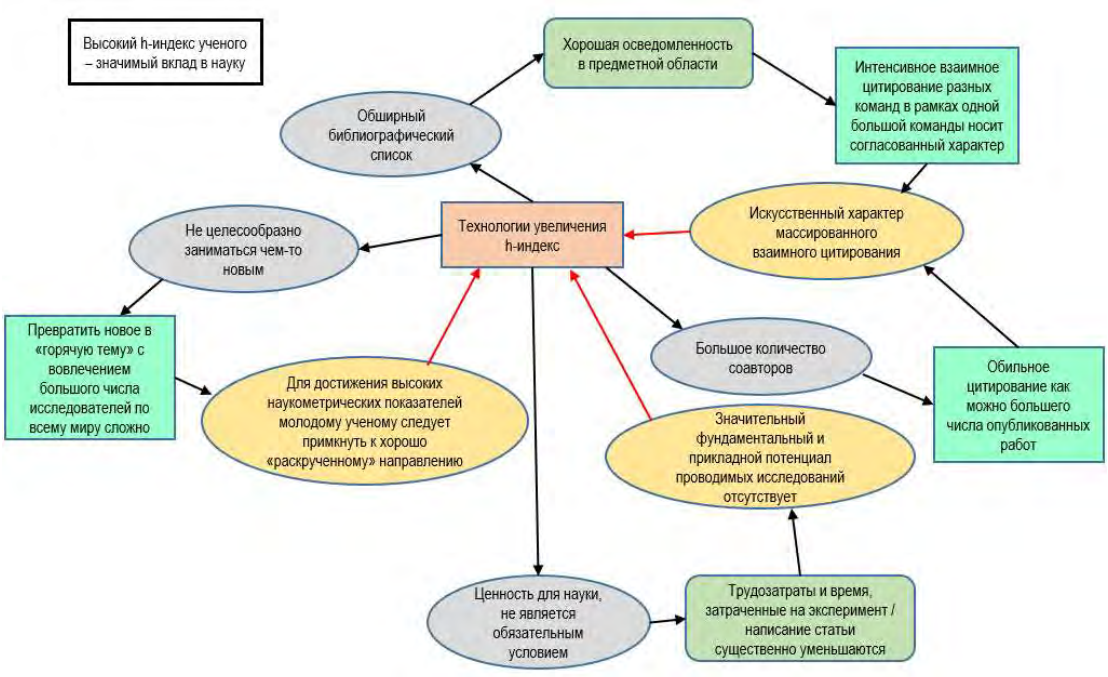


Рис. 4. Имитация науки в результате использования h-индекса для оценки деятельности научных работников

Заключение

Оценка результатов научной деятельности – существенная часть научной деятельности и фактор повышения эффективности науки. Процедура этой оценки основана на индексировании в наукометрических базах данных. Основными показателями, которые определяет уровень значимости научного вклада в результате исследовательской деятельности, в РФ все еще

остаются импакт-фактор и h-индекс. В основе этих индикаторов лежит цитирование и публикационная активность. Однако высокая цитируемость и тем более множество публикаций не всегда отражают важность и влияние на конкретную предметную область, поэтому актуальным продолжает оставаться поиск новых методик оценки вклада в науку. Например, диаграммы Beamplots дают более полную статистики цитирования: год первой публикации, спад публикационной активности, карьерный рост [8]. Влияния научной статьи дополнительно можно оценить с помощью альтметрик. Объективность импакт-фактора и h-индекса не всегда устойчива. Цитирование демонстрирует неполную картину оценки научной продуктивности, и часто неправильно используется. Поскольку результаты измерения качества работы исследователя влияют на его научную карьеру, особенно важно проводить тщательную экспертизу его деятельности, применяя правильные научные методы, и проводить новых наукометрические исследования.

Список используемых источников

1. Москалева О. В. Научные публикации как средство коммуникации, анализа и оценки научной деятельности // Руководство по наукометрии: индикаторы развития науки и технологии. Екатеринбург: Изд-во Урал. ун-та, 2014. С. 110–163.

2. Адлер Р., Эвинг Д., Тейлор П. Статистики цитирования // Игра в цыфирь, или как теперь оценивают труд ученого (сб. ст. о библиометрике). М.: МЦНМО, 2011. С. 6–38.

3. Чеботарев П. Ю. Наукометрия: как с её помощью лечить, а не калечить? // Управление большими системами: сборник трудов. Специальный выпуск 44: «Наукометрия и экспертиза в управлении наукой». 2013. № 44. С. 14–31.

4. Власова В. В., Гохберг Л. М., Дьяченко Е. Л. и др. Российская наука в цифрах / Нац. исслед. ун-т «Высшая школа экономики». М.: НИУ ВШЭ, 2018.

5. Имаев В. Технологии увеличения индекса Хирши и развитие имитационной науки // В защиту науки. Комиссия РАН по борьбе с лженаукой и фальсификацией научных исследований. Бюллетень № 17. М., 2016. С. 38–52.

6. Tagiew, R.; Ignatov, D. I. Behavior Mining in h-index Ranking Game // CEUR Workshop Proceedings. 2017. Vol. 1968. Pp. 52–61.

7. Hirsch, J. E. An index to quantify an individual's scientific research output // Proceedings of the National Academy of Sciences of the United States of America. 2005. Vol. 102. Iss. 46. Pp. 16569–16572. https://doi.org/10.1073/pnas.0507655102.

8. Brito, R.; Navarro, A. R. The inconsistency of h-index: A mathematical analysis // Journal of Informetrics. 2021. Vol. 15. Iss. 1. https://doi.org/10.1016/j.joi.2020.101106.

9. Haunschild, R.; Bornmann, L.; Adams, J. R package for producing beamplots as a preferred alternative to the h index when assessing single researchers (based on downloads from Web of Science) // Scientometrics. 2019. Vol. 120. Pp. 925–927. https://doi.org/10.1007/s11192-019-03147-3.

10. Орлов А. И. Наукометрия и управление научной деятельностью // Управление большими системами: сборник трудов. Специальный выпуск 44: «Наукометрия и экспертиза в управлении наукой». 2013. № 44. С. 538–568.

Статья представлена научным руководителем,
доктором технических наук, профессором М. В. Буйневичем.

УДК 004.85:004.056.57
ГРНТИ 81.93.29

ПРИМЕНЕНИЕ РЕКУРРЕНТНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ КЛАССИФИКАЦИИ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

А. Н. Цибуля, В. В. Фадеев

Академия Федеральной службы охраны Российской Федерации

В работе рассмотрена возможность применения рекуррентных нейронных сетей архитектуры LSTM для решения задач классификации вредоносного программного обеспечения, аналитически описана структура сети и представлена структурная схема модуля LSTM сети. Целью работы является повышение эффективности проведения компьютерно-технической экспертизы при анализе вредоносного ПО.

информационная безопасность, классификация вредоносных программ, нейронные сети.

Классификация является распространенной задачей при анализе вредоносного программного обеспечения в ходе проведения компьютерно-технической экспертизы. Обычным способом классификации вредоносного кода является экспертная оценка похожести антивирусных образцов квалифицированным членом группы реагирования на инциденты информационной безопасности. Основная проблема данного метода заключается в сложности анализа полиморфных и метаморфных вирусов.

Таким образом, разработка метода автоматической классификации вирусов позволит повысить эффективность проведения расследований инцидентов информационной безопасности, связанных с действием различного вредоносного ПО. В качестве признака классификации в работе будет использоваться последовательность вызовов API-функций, получаемая в ходе динамического анализа вредоносного ПО в изолированной программной среде. Для достижения этой цели предлагается использовать методы машинного обучения, которые показали хорошие результаты при решении задач бинарной классификации [1]. Это обуславливается большим количеством образцов известного на данный момент вредоносного ПО, а также тем фактом, что новые модификации вирусов используют сходные технологии.

Основная задача методов машинного обучения состоит в определении зависимости между исследуемыми данными и выявляемыми признаками вредоносности [2]. Эффективность этих методов зависит от характера обнаруживаемых признаков, подбора входных данных и качества обучения,

Основные методы классификации ВПО при помощи машинного обучения представлены на рис. 1.

Рис. 1. Методы классификации ВПО при помощи машинного обучения

В случае наличия большого объема данных, глубокое обучение, которое является подобластью машинного обучения, позволяет достичь более точных результатов, чем традиционные алгоритмы, с использованием моделей искусственных нейронных сетей (ИНС), таких как рекуррентные нейронные сети (РНС). Основная отличительная особенность РНС от других нейронных сетей, – это образование прямых циклов между нейронами. Это обеспечивает сеть временной обработкой и обучением последовательности путем создания внутренних состояний. Эти особенности и сложность РНС требуют большого количества времени для обучения сети, а также наличия больших объемов памяти.

Внутренние состояния в РНС позволяют запоминать информацию о предыдущих активированных нейронах и выполнять расчеты сети с учетом обратной связи между элементами с каждым шагом времени. Пусть для одного скрытого слоя РНС определен шаг времени *t, i*(*t*) и *o*(*t*) как входные и выходные векторы соответственно, *h(t)* как скрытый вектор, соответствующий скрытому слою, f_h и f_0 как функции активации скрытого слоя и выходного слоя соответственно, P_{ih} – весовая матрица между входным слоем и скрытым слоем, P_{hh} – весовая матрица между скрытым слоем и очередным скрытым слоем, а P_{ho} – весовая матрица между скрытым слоем и выходным

слоем. Тогда выражения, описывающие функцию активации скрытого слоя и функцию выхода будут иметь следующий вид:

$$h(t) = f_h\left(i(t)P_{ih} + h(t-1)P_{hh}\right), \quad (1)$$

$$o(t) = f_o\left(h(t)P_{ho}\right). \quad (2)$$

Для решения задачи классификации вредоносного ПО была выбрана нейронная сеть LSTM – сети с долгосрочной кратковременной памятью, являющимися подтипом РНС. Такой выбор обуславливается изначальной предрасположенностью таких сетей к анализу последовательностей событий. Каждое последующее действие программы или пара таких действий имеет зависимость от уже выполненных предыдущих действий. Определенные совокупности таких последовательностей могут отличить вредоносное ПО от невредоносного. При помощи сети с долгой краткосрочной памятью можно выявить зависимости данных при их временном разделении, что подходит для данной задачи.

На рис. 2 изображена базовая структура модуля LSTM сети.

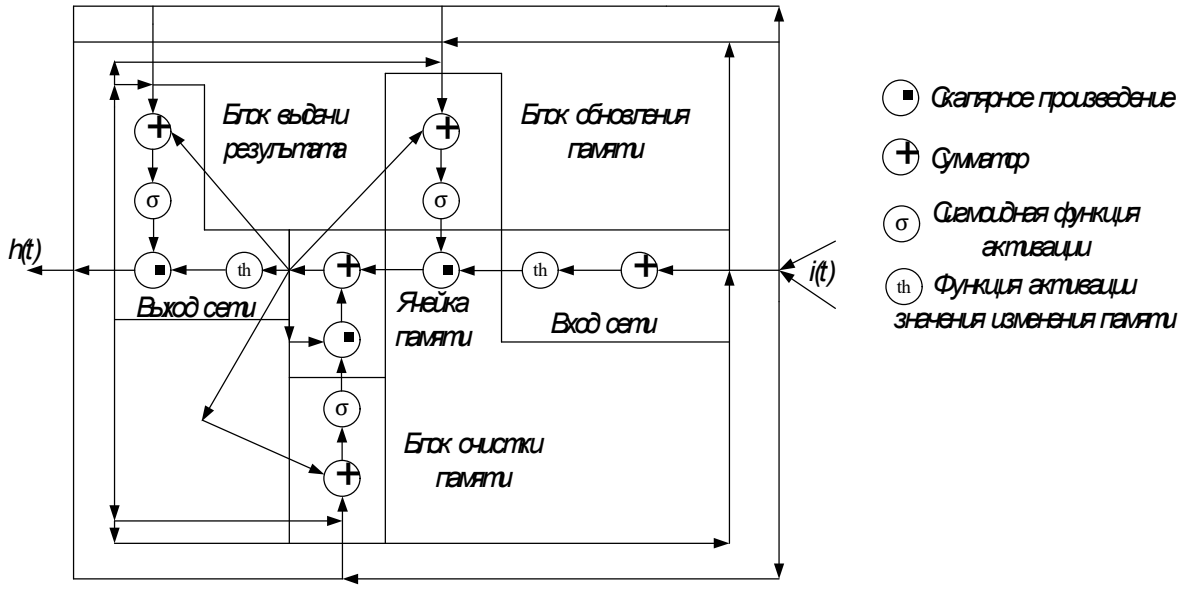


Рис. 2. Архитектура модуля LSTM сети

В состав LSTM-модуля входят 3 блока, или вентиля: блок обновления памяти (входной вентиль), блок выдачи результата (выходной вентиль) и блок очистки памяти (вентиль забывания), контролирующие потоки информации на входах и на выходах памяти данных блоков. Данные вентили реализуются в виде логистической функции в целях вычисления значения в диапазоне [0; 1]. Умножив на это значение, можно получить разрешить, или наоборот, запретить прохождение потока информации внутрь и наружу

ячейки памяти. Например, входной вентиль контролирует меру вхождения нового значения в память, а вентиль забывания контролирует меру сохранения значения в памяти. Функцией выходного вентиля является осуществление контроля меры того, в какой степени значение, находящееся в памяти, используется при расчёте выходной функции активации для блока. Существуют такие реализации, в которых входной вентиль и вентиль забывания воплощаются в виде единого вентиля. Идея заключается в том, что старое значение следует забывать тогда, когда появится новое значение, достойное запоминания [3].

Опишем аналитически модель LSTM сети. Пусть σ – логистическая функция, *y*, *x*, *w* и *z* – вентиль забывания, входной вентиль, выходной вентиль и векторы активации ячеек соответственно, P_{ix} – весовая матрица между входным вектором и входным вентилем, P_{hx} – весовая матрица между скрытым слоем и входным вентилем, P_{zx} – весовая матрица между вектором ячейки и входным вентилем, P_{iy} – весовая матрица между входным вектором и вентилем забывания, P_{hy} – весовая матрица между вектором скрытого слоя и вентилем забывания, P_{zy} – весовая матрица между вектором ячейки и вентилем забывания, P_{iz} – весовая матрица между входным вектором и ячейкой, P_{hz} – весовая матрица между вектором скрытого слоя и ячейкой, P_{iw} – весовая матрица между входным вектором и выходным вентилем, P_{hw} – весовая матрица между вектором скрытого слоя и выходным вентилем и P_{zw} – весовая матрица между вектором ячейки и выходным вентилем, тогда зависимости примут вид, представленный в формулах (3), (4), (5), (6) и (7):

$$x(t) = \sigma\left(P_{ix} i(t) + P_{hx} h(t-1) + P_{zx} z(t-1) + b_x\right), \tag{3}$$

$$y(t) = \sigma\left(P_{iy} i(t) + P_{hy} h(t-1) + P_{zy} z(t-1) + b_y\right), \tag{4}$$

$$z(t) = y(t) z(t-1) + x(t) \tanh\left(P_{iz} i(t) + P_{hz} h(t-1) + b_z\right), \tag{5}$$

$$w(t) = \sigma\left(P_{iw} i(t) + P_{hw} h(t-1) + P_{zw} z(t) + b_w\right), \tag{6}$$

$$h(t) = w(t) \tanh\left(z(t)\right). \tag{7}$$

Сигмоидная функция активации всегда присутствует в модуле LSTM и описывается формулой (8), гиперболическая функция активации представлена формулой (9), а логистическая функция выражена формулой (10), где *L* – максимальное значение кривой, x_0 – значение середины сигмоиды, а *k* – скорость логистического роста или крутизна кривой.

$$S(x) = \frac{e^x}{\left(e^x + 1\right)}, \tag{8}$$

$$\tanh(x) = \frac{\left(1 + e^{2x}\right)}{\left(1 - e^{-2x}\right)}, \tag{9}$$

$$f(x) = \frac{L}{\left(1 + e^{(-k(x - x_0))}\right)}. \tag{10}$$

Таким образом, аналитически была описана модель LSTM-сети, предназначенной для классификации вредоносного ПО. На основе разработанной модели возможно построение автоматизированных систем анализа файлов, предназначенных для проведения расследований инцидентов информационной безопасности.

Список используемых источников

Gardiner, J.; Nagaraja, S. 2016. On the security of machine learning in malware c&c detection: A survey. ACM Computing Surveys (CSUR) 49, 59

Подпружников Ю. В. Классификация методов обнаружения неизвестного вредоносного программного обеспечения // Современные тенденции технических наук : материалы I Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). Уфа : Лето, 2011. С. 22–25. URL: https://moluch.ru/conf/tech/archive/5/1133/ (дата обращения 30.03.2021).

Долгая краткосрочная память // Википедия. [2021]. 12.01.2021. URL: https://ru.wikipedia.org/?curid=6768734&oldid=111677373 (дата обращения 12.01.2021).

УДК 519.17
ГРНТИ 27.45.17, 28.17.19

МАТЕМАТИЧЕСКИЕ МОДЕЛИ РИСКОВ И СТРУКТУРНЫХ РИСК-ПАРАМЕТРОВ ИНФРАСТРУКТУРНЫХ ПРОЕКТОВ

К. А. Фролова, А. В. Шестаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается проблема снижения рисков организации сложных проектов и управления ими по результатам мониторинга структурных риск-параметров многосценарных систем. Обосновывается математический аппарат формального описания процедур управления рисками инфраструктурных проектов на примере взаимоувязанных сложных систем телекоммуникационной и транспортной региональной

инфраструктуры. Анализируются традиционные способы построения моделей сложности систем, представленных в виде графа, способы различения расположения графов. Предложены проактивные процедуры управления сложными проектами на основе мониторинга структурных риск-параметров многосценарных систем.

математические модели рисков, сложный проект, графовые модели систем.

Введение

Процессы создания, развития и совершенствования разнородной инфраструктуры и ее элементов, увязанные «дорожными картами», относятся к реализации сложных проектов. Источниками рисков реализации сложных проектов являются не только временные издержки выполнения мероприятий и работ «дорожной карты», а также нереализуемость элементов или параметров инфраструктуры, из-за их зависимости от состояния других проектов, что выявлено в процессе реализации. Задача заблаговременного определения и формального описания таких критических точек – рисков сложных проектов – является достаточно актуальной.

Сущность проблемы

Группа взаимоувязанных сложных проектов, на примере Санкт-Петербурга, содержит:

– проект развития телекоммуникационной инфраструктуры до 2030 года, в рамках концепции отрасли связи на среднесрочную перспективу;

– проект развития транспортной инфраструктуры, в форме комплексной схемы организации дорожного движения до 2033 года;

– проект поэтапного ввода в эксплуатацию высокоавтоматизированного транспорта в России и ряд других.

В основе проектов – реализация инфраструктуры, системы, подсистемы и элементы которой могут находиться во взаимном проникновении (диффузии) за счет общности инфраструктурных элементов (подсистем), а также объективно существующих эмерджентных характеристик, которые получены по результатам выполнения мероприятий других проектов, что и является причиной рисков нереализуемости проектов. Риски по каждой подзадаче отдельно взятого проекта имеют стохастическое влияние на реализуемость комплексного проекта в целом.

Проблематичность управления рисками инфраструктурных проектов значительно усугубляется при возрастании степени диффузионного структурного проникновения различных подсистем (элементов), рисках формирования несвязанных элементов и фрагментов, отсутствии механизмов многосценарных стратегий управления проектами.

Существующая практика федеральных, региональных и отраслевых инфраструктурных проектов выявила востребованность в новых моделях координации и управления структурными параметрами систем, которые взаимообусловлены идентичностью объектов различных проектов и неоднородностью рисков.

Решение

Традиционные подходы к определению рисков проектов, например, в [1], основаны на определении величины превышения затрат времени на выполнение проекта как случайной величины и описании распределения вероятности выполнения проектов в срок и с превышением времени выполнении проектов в каждой из рассматриваемых выборок. Превышение затрат времени проекта прогнозируется исходя из того, что вероятность выполнения проекта в срок или с нарушением установленного заказчиком срока подчинена нормальному закону распределения. Пример статистических плотностей распределения случайных величин четырех типов систем проектов представлен на рис. [1]. Традиционные подходы не позволяют выявлять источники рисков невыполнения проектов и критические элементы инфраструктуры.

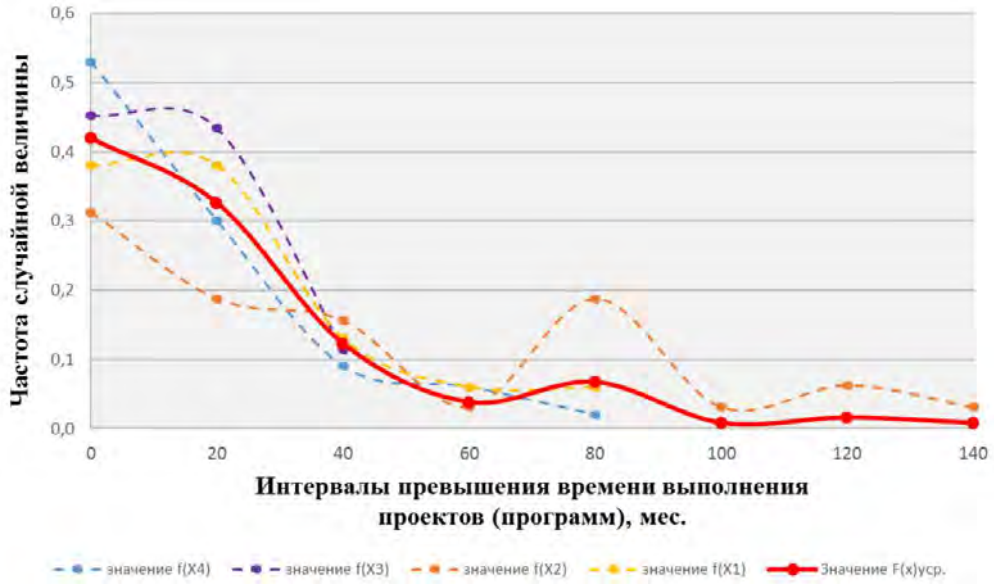


Рис. Плотности распределения случайных величин проектов [1]

Реализация любого сложного проекта во времени, как показано в [2], является задачей достройки графа на очередном этапе создания (развития) инфраструктуры. Главным для ее решения являются процедуры формирования первоначального графа (нулевого) или графа первого этапа (исходного фрагмента системы) с соответствующими пространственными данными и атрибутами вершин и ветвей графа, применительно

к инфраструктурному проекту. Исходным графом является граф полномасштабной системы. Полномасштабная система является результатом проектирования, объектом и целью реализации сложного проекта. За счет применения методов спарсификации исходного графа формируют сжимающие последовательности геосемплов (подграфов), которые определяют необходимый и достаточный уровень (состав) графа первого этапа.

Изменение условий решения задачи формирования графа очередного этапа развития, за счет введения в состав объектов инфраструктуры оборудования нового типа, устройств и средств, реализующих сквозные цифровые технологии (перспективные инфотелекоммуникационные технологии), повлечет изменение технических возможностей и характеристик системы, что обусловливает необходимость решения задач модификации процедур достройки графа.

Решение частной задачи адаптации сложных проектов к изменяющимся условиям предложено в [3] на основе модели управления параметрами систем многосценарных сложных проектов и процедуры ситуационного управления с учетом функциональных элементов модели системы ситуационного управления объектом проектирования. На примере подсистемы управления создаваемой инфраструктуры в [3] представлены частные процедуры уточнения структурных параметров по результатам натурных испытаний и динамического управления сложным проектом.

Анализ выполняемых в настоящее время проектов показывает, что ввиду значимости рисков нереализации отдельных этапов имеет место задача определения сложности моделей систем. Задача может быть сведена к графовым моделям для определения вклада фрагментов, таких как вершины, ребра, цепи, пути и другие, в общую сложность графа. В основе исследования сложности графовых моделей систем принята теория структурного сходства систем.

Величина вклада отдельных фрагментов системы в ее общую сложность определяет риски, связанные с невыполнением отдельных этапов сложных проектов, что может привести к разрыву графа на несвязные графы и, как следствие, повлечь риски нереализации отдельных этапов других сложных проектов, связанных общими элементами или характеристиками.

Традиционными способами определения сложности систем, представленных графами, являются построение модели на основе теоретико-информационных индексов вершин графа, в которых сложность связана с симметрией графов, моделей сложности, имеющих в основе мультииндексы, вычисление функции сложности, значение которой равно числу остовных деревьев графа, а также построение матричных моделей сложных систем.

Матричная модель сложности орграфа G, которая позволяет определить сложность системы на основе вклада ее фрагментов заданного вида

в общую сложность, как представлена в [4], может быть применена для целей настоящего исследования. Матрица относительных вкладов фрагментов орграфа G в его сложность строится на основе матрицы достроек фрагментов $EM * (\frac{G}{F^l} \subseteq B)$:

$$MIRC\left(F^l \subseteq B(G)\right) = \left\| irc(\frac{f_i^t}{b_j}) \right\|, i = 0 \dots k+4; j = 1 \dots kl+3, \quad (1)$$

где F^l – множество помеченных фрагментов;

B – базис структурных дескрипторов, относительно которого характеризуется сложность графа.

Значения элементов матрицы вычисляются по формуле:

$$irc\left(\frac{f_i^t}{b_j}\right) = \frac{m_{ij}}{Sw\left(\frac{F^l}{b_j}\right)} * \frac{ISC\left(b_j\right)}{ISC\left(\frac{G}{B}\right)}, \quad (2)$$

где $ISC(b_i)$ – индекс структурной сложности элементов базиса.

Относительный вклад f_i^t в общую сложность орграфа при использовании базиса B определяется:

$$iirc\left(\frac{f_i^t}{B}\right) = \frac{1}{ISC\left(\frac{G}{B}\right)} \sum_{j=1}^{kl} m_{ij} \frac{ISC\left(b_j\right)}{Sw\left(\frac{F^l}{b_j}\right)}. \quad (3)$$

Предложенные модели вклада фрагментов в общую сложность орграфа должны быть включены в виде дополнительных процедур ситуационного управления, которые представлены в [3].

Заключение

Для нужд органов исполнительной власти такого субъекта федерации, как Санкт-Петербург, задействовано более 70-ти информационных систем, которые относятся к государственным, обеспечивают контроль и мониторинг исполнения сложных проектов (государственных и региональных программ, проектов и контрактов), а на уровне информационно-аналитической системы Санкт-Петербурга – их общую консолидированную координацию и управление. Пространство моделей рисков должно соответствовать принятой для сложного проекта системе декомпозиции его компонент по классификационным признакам. Модели структурных риск-параметров определяются моделями сложности фрагментов графов инфраструктурного проекта. Управление рисками и структурными риск-параметрами инфраструктурных проектов реализуется посредством процедур динамического

управления и комбинированных испытаний при валидации управляющих воздействий.

Список используемых источников

1. Месхи Н. Г., Дудорова Н. А. Модель показателя превышения времени выполнения сложного инновационного проекта для решения задачи управления рисками при планировании работ // Радионавигация и время. 2020. № 5 (13). С. 85–99.
2. Шестаков А. В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. СПб.: ГУАП, 2016. 325 с.
3. Frolova, K. A.; Shestakov, A. V. Models for Managing the Structural Parameters of Complex Project Systems // The Way of Science International scientific journal. 2020. № 9 (79). Pp. 35–42.
4. Кохов В. А., Кохов В. В. Метод решения задачи различения орграфов на основе сложности // Бизнес-информатика. 2011. № 1 (15). С. 11–23.

УДК 004.056.5
ГРНТИ 81.93.29

ОСНОВНЫЕ ИСТОЧНИКИ ТЕРМИНОЛОГИЧЕСКОЙ БАЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В. С. Хорошенко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье исследуются основные источники терминологической базы информационной безопасности. Внимание сфокусировано на выбранном как системообразующем термине информационная безопасность. Рассматривается тема причин, сформировавших текущее состояние. Подсвечивается актуальность проблемы и делаются выводы относительно направления развития.

информационная безопасность, кибербезопасность, термин, стандарт.

В 2020 г. короновирус и пандемия внесли свои коррективы и погрузили мир в оффлайн. Практически все сферы жизни: бизнес, образование, медицина, шоппинг, досуг «ушли на удаленку», что обострило проблему информационной безопасности (ИБ). За 2020 год количество киберпреступлений выросло на 94,6 %.

Проблема обеспечения ИБ стала как никогда стратегически важной. По причине того, что в основе любого процесса лежит терминологическая

база, важно проанализировать основные источники терминологической базы ИБ.

Для этого рассмотрим следующие источники:

1. Нормативно-правовые акты.

В качестве примеров приведем Доктрину ИБ РФ и Конвенцию об обеспечении международной информационной безопасности.

В Доктрине [1] дается определение ИБ РФ как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие РФ, оборона и безопасность государства». Проведем ретроспективный анализ. Доктрине от 2016 г. предшествовала утратившая силу Доктрина от 09.09.2000 г., из которой в новый документ была перенесена модифицированная добавлением основных конституционных постулатов основа определения «состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства». Проследим истоки данной формулировки и обратим внимание на утративший силу Закон РФ от 05.031992 г. N 2446-I «О безопасности», из которого был взят каркас определения безопасность как «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз».

Это был хронологически первый нормативно-правовый акт, принятый в непростое время в результате совместной работы Комиссии по разработке предложений по статусу, структуре и порядку деятельности Совета Безопасности РСФСР и комитетов Верховного Совета РФ по безопасности и по законодательству. Закон стал основополагающим, задав тренд и «моду» определения безопасности. Анализируя определение, можно сделать вывод, что термин построен на определении из толкового словаря Ожегова, характеризующего безопасность как «состояние, при котором не угрожает опасность, есть защита от опасности» [2], т. е. защищенности, являющейся близким синонимом безопасности.

Подведя итоги, как мы видим, Доктрина является совокупностью официальных взглядов. И хотя основная цель Доктрины носит политическую окрашенность, она выступает базой «правового, методического, научно-технического и организационного обеспечения ИБ РФ» [1], что мы неоднократно отметим при дальнейшем анализе документов.

Так, в Конвенции об обеспечении международной ИБ (концепция) в основу определения ИБ положено знакомое нам из Доктрины «состояние защищенности интересов личности, общества и государства от угроз деструктивных и иных негативных воздействий в информационном пространстве».

2. Государственные стандарты России.

Для начала рассмотрим два Госта, подготовленных ФСТЭК в 2005 г. и введенных в действие в 2006 г., дающие два идентичных определения, перекликающихся с рассмотренным определением из Доктрины:

Безопасность информации – состояние защищенности информации, при котором обеспечивается ее конфиденциальность, доступность и целостность [3]. Разработан совместно с Техническим комитетом по стандартизации ТК 362 «Защита информации».

Безопасность информации (данных) - состояние защищённости информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность [4]. При этом интересно обратить внимание на предыдущую версию ГОСТ Р 50922-96, разработанную Техническим комитетом по стандартизации «Защита информации» ТК 362Р в 1996 г. и введенную в действие в 1997 г., дававшую иное определение защита информации как «деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию».

В основе следующего рассматриваемого ГОСТа лежит перевод на русский язык англоязычной версии стандарта, подготовленный ФСТЭК и ООО «НПФ «Кристалл». В [5] дано определение ИБ как «свойство информации сохранять конфиденциальность, целостность и доступность. Примечание – кроме того, данное понятие может включать в себя также и свойство сохранять аутентичность, подотчетность, неотказуемость и надежность» Как указано в тесте ГОСТа, что настоящий стандарт идентичен международному стандарту ИСО/МЭК 27001:2005 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (ISO/IEC 27001:2005 «Information technology – Security techniques – Information security management systems – Requirements», IDT).

Проанализировав различные ГОСТы, мы выявили, что несмотря на одинаковую декларируемую цель документов разные исполнители (разработчики) создавали несогласованые, непоследовательные документы, не придерживаясь общей стратегии.

3. Международные стандарты ИСО (ISO).

Рассматривая последний ГОСТ, мы отметили, что он по своей сути составляет перевод международного стандарта Международной организации по стандартизации, миссия которой предоставлять готовые решения для различных стран с целью облегчить международное взаимодействие и способствовать совместимости. Все стандарты доступны на английском и французском языках. Сама Организация заявляет, что определения даны в максимально простой для перевода форме, не несущей двусмысленные толкования. В ходе исследования была проведена экспертиза, показавшая,

что структура определений вызывает сложности толкования даже у носителей английского языка с академическим бэкграундом.

Международный стандарт, на который идет отсылка ГОСТа, был опубликован в 2005 г. и пересматривается каждые 5 лет. Действующая сейчас версия от 2013 г. с поправками от 2014 г. и 2015 г. Однако в данном стандарте вы не найдете терминов с определениями, на которые ссылаются в ГОСТе. Для целей данного стандарта применяются термины и определения, содержащиеся в родительском стандарте ISO/IEC 27000.

Стандарт впервые опубликован в 2009 г., пересматривался в 2012 г., 2014 г., 2016 г., действующая версия от 2018 г.

В [6] ИБ (Information security) представляется как сохранение конфиденциальности, целостности и доступности информации.

Если рассматривать все стандарты, объединенные под сводом серии 27000, то в отличие от российской действительности термины и определения едины и вынесены для удобства использования в вышеназванный стандарт.

4. Определения, вводимые научно-педагогическими сотрудниками в учебных материалах.

Та неоднозначность и многообразие определений, которое мы уже увидели, особо четко просматриваются в этом источнике. При этом научно-педагогические сотрудники едины в одном, что нет однозначного определения термина ИБ. Каждый вводит свое определение на основе Доктрины, Гостов и суждений. Часто можно встретить такое введение: под ИБ будем понимать, ИБ трактуется и т. д. В итоге профильные выпускники разных вузов приходят в практическую сферу обеспечивать ИБ с различным пониманием одного и того же понятия.

Приведем несколько примеров:

В [7] под ИБ понимают «защищенность информации и поддерживающей инфраструктуры».

В [8] трактуется «с одной стороны, как состояние защищенности человека, общества и государства в информационной сфере, а с другой - как результат деятельности по обеспечению ИБ».

В [9] рассматривают как «состояние защищенности».

В [10] понимают как «защищенность информации».

В [11] характеризуют как «такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой – ее функционирование не создает информационных угроз для элементов самой системы и внешней среды».

5. Определения, используемые бизнес-структурами.

Как мы увидим, следующие определения характеризуются как меры и мероприятия и отличаются практической направленностью продвижения

услуг и продуктов, предлагаемых бизнес-структурами. Рассмотрим крупнейших игроков InfoWatch и Kaspersky.

InfoWatch рассматривает обеспечение ИБ как меры по охране конфиденциальности информации и рекомендации по применению организационных мер и технических средств, направленных на защиту конфиденциальной информации.

Kaspersky рассматривает кибербезопасность как практику защиты компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от вредоносных атак.

Подводя итоги, мы сделали вывод, что категория ИБ – относительно молодое, в стадии развития и формирования понятие. Изучив определение ИБ в различных источниках, мы основательно подтвердили, что единого подхода нет, при этом можно выделить следующие векторы рассмотрения: состояние защищенности, свойство информации и мероприятия, направленные на обеспечение защиты.

Причины текущего состояния термина в РФ кроятся в следующем:

– множественное число организаций, вовлеченных и ответственных за выработку стандартов, при этом не согласующих друг с другом свою работу в этом направлении;

– отсутствие преемственности документов;

– локальное применение международного опыта;

– свободный перевод и интерпретация иностранных терминов и определений;

– ограниченность во времени на выработку стандартов;

– отсутствие аудита и актуализации документов;

– одновременное нахождение термина как в сфере влияния юриспруденции, так и информационных технологий.

Проанализировав основные источники, можно сделать еще и вывод, что разные источники (стейкхолдеры) рассматривают термин ИБ исходя из того уровня или уровней информационного пространства, в которых они оперируют. Здесь будет интересно перенести эти уровни на пирамиду Маслоу (пирамида потребностей). Это поможет наглядно увидеть на рис. как по аналогии со структурой потребностей человека выстраивается иерархия уровней кибербезопасности от обеспечения базовой безопасности до высокоуровневых категорий как глобальная устойчивость и защита прав человека.

Рис. Уровни обеспечения кибербезопасности [12]

Рассмотрев, как строилось понятие термина разными группами, в разное время, с разными концепциями и целями, выкристаллизовывается ряд вопросов:

1) Один термин трактуется неоднородно, как в целом, между группами, так и внутри одной и той же группы. Должно ли быть единое определение? Очевидный ответ – да, должно и нужно. Будет это Единый для всех уровней и групп или хотя бы в рамках одной группы термин?

2) Как создать такой универсальный единый категориальный аппарат?

Для предварительного ответа на первый вопрос, достаточно еще раз посмотреть информацию об информационных угрозах, а также допустить, что, как правило, нет четкой изоляции определенного уровня, как правило, одновременно затрагиваются несколько, что, безусловно, создает и ведет к рискам при разработке требований по ИБ государственными органами, корпорациями, некоммерческими организациями и другими стейкхолдерами, а также при их взаимодействии.

Поиску решений на эти вопросы с учетом полученного опыта будут посвящены наши дальнейшие работы.

Список используемых источников

1. Указ Президента Российской Федерации от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения 20.02.2021)

2. Толковый словарь Ожегова. URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения 20.02.2021)

3. Рекомендации по стандартизации. 50.1.056-2005. Техническая защита информации. Основные термины и определения. URL: http://docs.cntd.ru/document/1200044768 (дата обращения 20.02.2021)

4. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. URL: http://docs.cntd.ru/document/1200058320 (дата обращения 20.02.2021)

5. ГОСТ Р ИСО/ МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

Требования. URL: https://www.in-nov.ru/doc/standarti/gost_27001.pdf (дата обращения 20.02.2021)

6. ISO/IEC 27000:2018. Information technology – Security techniques – Information security management systems – Overview and vocabulary (Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и терминология). URL: https://www.iso.org/obp/ui/ #iso:std:iso-iec:27000:ed-5:v1:en (дата обращения 20.02.2021)

7. Галатенко В. А. Основы информационной безопасности: учеб. пос. 2-е изд. Москва: ИНТУИТ, 2016. 266 с.

8. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры / под ред. Т. А. Поляковой, А. А. Стрельцова. М.: Издательство Юрайт, 2016. 325 с. ISBN 978-5-9916-6799-9

9. Вострецова Е. В. Основы информационной безопасности: учебное пособие для студентов вузов. Екатеринбург: Изд-во Урал. ун-та, 2019. 204 с. ISBN 978-5-7996-2677-8

10. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. М.: ИД «ФОРУМ»: ИНФРА-М, 2011 416 с. ISBN 978-5-8199-0331-5, ISBN 978-5-16-003132-3

11. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. М.: Горячая линия-Телеком, 2004. 280 с.

12. ENISA overview of cybersecurity and related terminology. URL: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology (дата обращения 20.02.2021)

Статья представлена научным руководителем,
доктором технических наук, профессором М. В. Буйневичем.

УДК 004.418
ГРНТИ 20.15.05

АНАЛИЗ ПЛАТФОРМ ОБРАТНОЙ СВЯЗИ МЕЖДУ ГРАЖДАНАМИ И ОРГАНАМИ ВЛАСТИ В РАМКАХ НАЦИОНАЛЬНОГО ПРОЕКТА «ЦИФРОВАЯ ЭКОНОМИКА»

В. В. Черномырдин, А. А. Шиян

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Вопрос обратной связи между органами власти и обычными гражданами всегда стоял достаточно остро. Помимо очевидных вещей в виде писем с описанием проблем от граждан, постоянно внедряются новые способы и методы коммуникации. Одним из таких проектов является «Цифровая экономика», в рамках которого был реализован ряд инструментов, призванных помочь органам власти собирать обратную связь от

граждан, обратив таким образом внимание на действительно важные проблемы. При этом обратная связь собирается не только по проблемам, но и по предложениям, правда несколько другими инструментами.

государство, граждане, обратная связь, платформы, разработка.

В современном мире огромную роль играет не только сам факт возможности передачи информации, но и скорость этой передачи. Зачастую у граждан возникают проблемы, требующие безотлагательного решения, но в силу устоявшейся системы и её несовершенства, эти обращения теряются, не принимаются во внимание, либо реакция приходит тогда, когда в ней уже нет смысла.

Нашим государством было принято решение о создании единого «окна», по которому будут поступать обращения граждан. Реализация данной платформы была частью проекта «Цифровая экономика», стартовавшего в 2019 году. Подразумевалось создание интегрированного с «ГосУслугами» сервиса, способного по самым разным точкам агрегировать обращения и распределять их по органам власти, которые могли бы помочь или вовремя отреагировать на обращения граждан. Плановой датой реализации данного проекта должен был стать 2020 год и его начало, однако, ввиду ряда причин, система была запущена чуть позже и не везде.

Силами команд разработчиков данной системы были проведены закрытые тестирования в рамках некоторых городов и регионов, которые позволили получить дополнительную информацию по доработке. Сейчас подобная система реализована на официальных страницах большинства регионов нашей страны, но грамотное взаимодействие органов власти и этой системы ещё требует доработки. Так для центрального региона и его областей система уже получила положительный отклик граждан, так как время на обработку обращений существенно сократилось (в Нижегородской области на 30%), при этом если брать регионы западнее, то тут уже ситуация иная.

Так, в Алтайском крае данная система пока еще не была запущена, и для работы с гражданами преимущественно используются бумажные носители (информация из отчета по Алтайскому краю) [1], при этом существуют ресурсы по работе с инициативами (например, алтайпредлагай.рф). Анализ одной из таких платформ показывает, что сбор инициатив граждан проходит на конкурсной основе, после чего наиболее удачные заявки отбираются и финансируются. Это позволяет обратить внимание местной администрации на наиболее важные и нужные проекты. На самой платформе представлена интерактивная карта, которая отображает все реализованные проекты через эту платформу, с возможностью узнать подробнее (рис. 1).

Однако и тут есть недостатки. Данная платформа не подразумевает возможность быстрой обратной связи для граждан по бытовым проблемам (ямы на дорогах, проблемы с электричеством и др.).

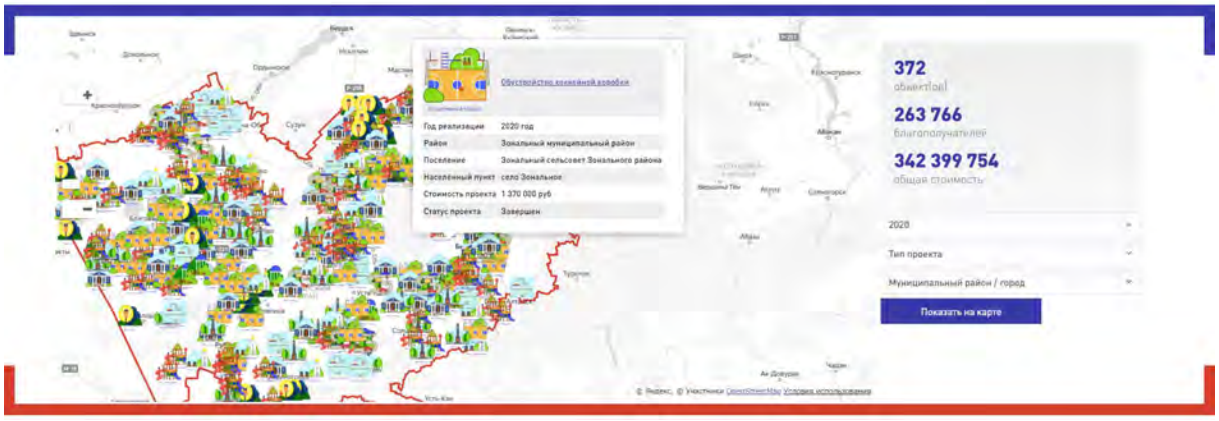


Рис. 1. Интерактивная карта инициатив

Рассмотрим другой регион, Вологодская область, тут реализован проект Гражданин35, который направлен на развитие региона и призван улучшить коммуникацию между гражданами и органами власти [2]. Данная система уже максимально похожа на то, что реализуется в рамках портала «ГосУслуги» и даже обладает рядом преимуществ. Главным из них является наглядность, ведь все проблемные зоны отображены на карте (на главной странице), а также у каждой проблемы есть свой статус и возможность обсуждения. Кроме того, отдельная проблема обладает рейтингом, что позволяет повысить внимание органов власти на какую-то конкретную проблему. Актуальность данной системы подтверждается тем, что тут ежедневно выкладываются новые проблемы. Все они, в основном, носят бытовой характер, но есть и крупные. Интерфейс системы представлен на рис. 2.

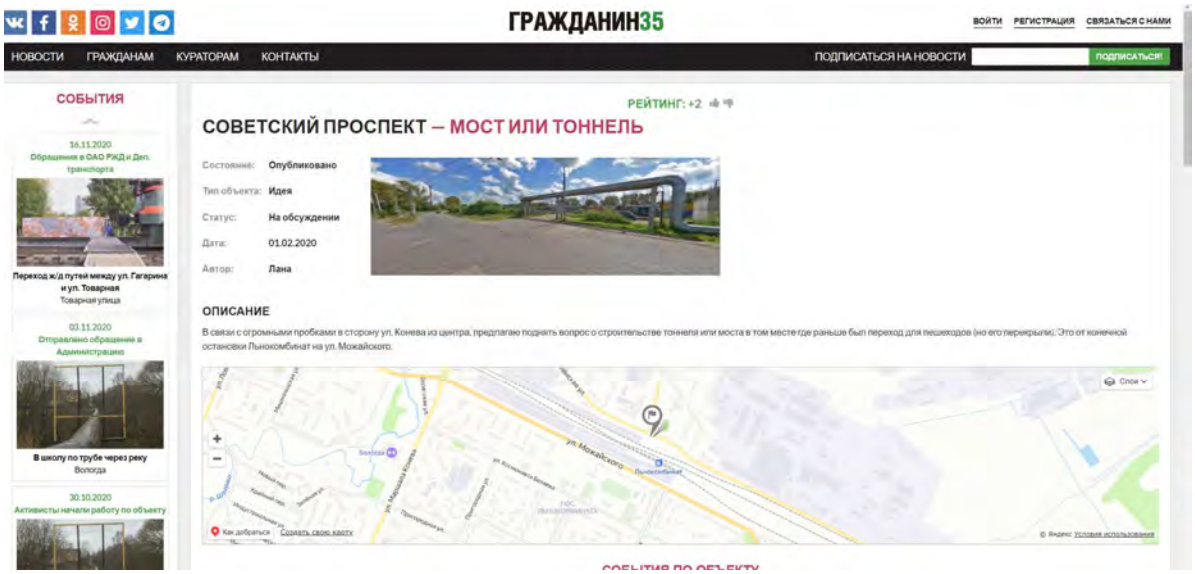


Рис. 2. Платформа Гражданин35

Другим интересным проектом в области обратной связи между гражданами и органами власти является «Умный Город» в Воронежской области [3]. Данный проект представляет собой интерактивную платформу для голосований по выбранным заранее темам. Здесь можно выразить свое мнение на ту или иную проблему, что позволяет органам местной власти корректировать те или иные проекты. Однако, платформа не представляет функционала, аналогичного предыдущим двум. Интерфейс платформы на рис. 3.

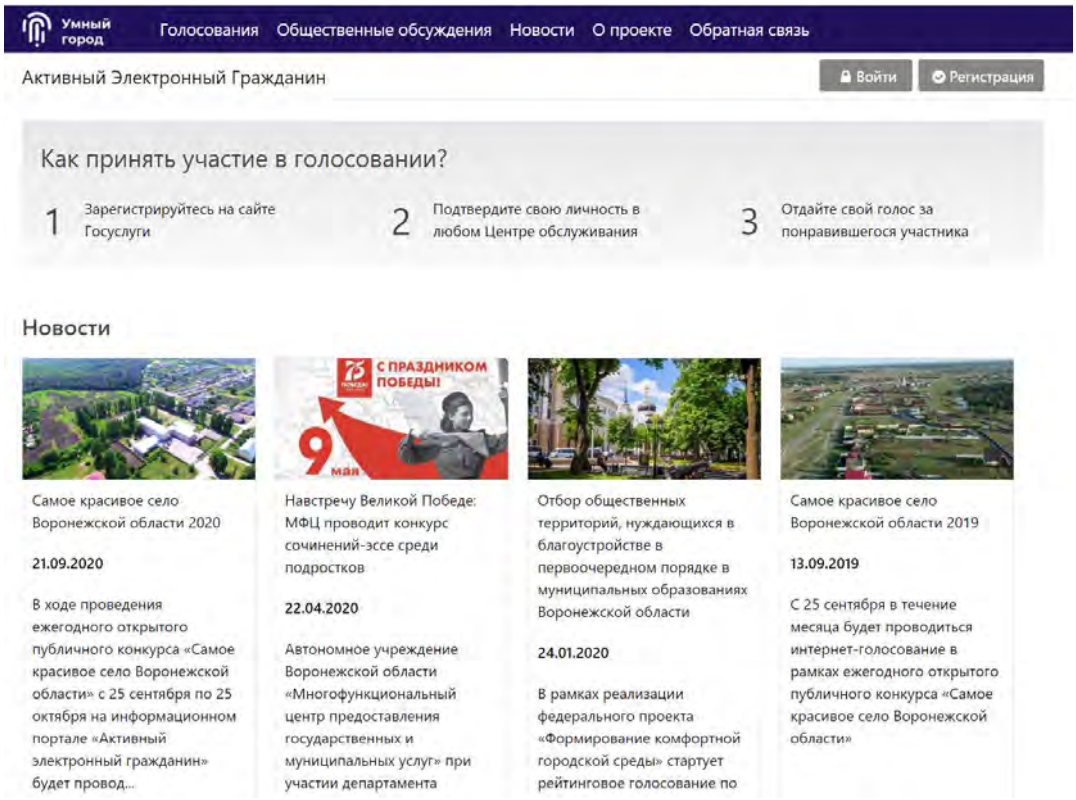


Рис. 3. Платформа «Умный город»

Рассмотренные проекты являются лишь малой частью того, что еще есть в регионах. Каждый из проектов обладает уникальным набором функциональных возможностей. Где-то эти возможности шире, где-то наоборот. В каждом регионе нашей страны найдутся проекты по обратной связи с органами власти, ведь это действительно важно и волнует людей сегодня. Все хотят быть услышанными, многие нуждаются в помощи [4].

Реализация «единого окна» в рамках платформы «ГосУслуги», однозначно сможет улучшить ситуацию во всех регионах, однако на текущий момент эта реализация представляет собой небольшой виджет, который размещается на сайтах правительства или администрации, куда можно отправить свое обращения, предварительно авторизовавшись. Нельзя сказать, что это решит все проблемы, ведь помимо проблем у граждан есть и предложе-

ния, так что в перспективе хотелось бы увидеть расширение данного «единого окна» и создания единой платформы взаимодействия граждан и орган власти со всеми нужными функциональными возможностями, которые так успешно реализованы в других проектах правительства или самих граждан.

Список используемых источников:

1. Алтай-Предлагай // Проект поддержки местных инициатив в Алтайском крае. URL: https://алтайпредлагай.рф.

2. Гражданин35 // Дмитрий Тарасов. URL: https://гражданин35.рф

3. Умный город // Департамент цифрового развития Воронежской области. URL: https://e-active.govvrn.ru/

4. Сервисы обратной связи с населением в регионах России // Comnews. URL: https://www.comnews.ru/content/205825/2020-04-27/2020-w18/servisy-obratnoy-svyazi-na-seleniem-regionakh-rossii

УДК 621.391; 621.395; 004.738.5
ГРНТИ 49.01.21

МЕТОДОЛОГИЯ ИССЛЕДОВАНИЙ ЛИЦЕНЗИРОВАНИЯ ИНТЕРНЕТ-СЕРВИСОВ ПЕРЕДАЧИ ГОЛОСОВОЙ ИНФОРМАЦИИ В ТЕЛЕФОННУЮ СЕТЬ ОБЩЕГО ПОЛЬЗОВАНИЯ

А. В. Шестаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются проблемы обеспечения и организации передачи голосовой информации в телефонную сеть общего пользования посредством интернет-сервисов. Анализируются существующие подходы к разрешению проблем регулятора, операторов связи и пользователей в правовой и технической сфере, с учетом различных влияющих факторов, условий и противоречий. Предложены методологические и методические подходы исследований лицензирования интернет-сервисов передачи голосовой информации в телефонную сеть общего пользования.

передача голосовой информации, интернет-сервисы, телефонная сеть.

Введение

Изучение организации и обеспечения бизнес-процессов операторов связи в рамах общеобразовательных программ вузов, основано преимущественно на исследовании технических аспектов. Вместе с тем, нормативно-

правовым (регуляторным) и экономическим аспектам уделяется меньше внимания и вне комплексного взаимоувязанного рассмотрения с техническими. Однако в сложных условиях постковидной экономики тенденции, например, нетрадиционной миграции передачи голосовой информации (ПГИ) перспективных сетей в унаследованные, кардинальное изменение информационных тяготений пользователей сетей связи, развернутых с применением различных технологий, обостряет проблемы междисциплинарного и комплексного изучения новых сущностей бизнес-процессов операторов связи, и обусловливает необходимость разрешения с учетом заинтересованных сторон [1].

Проблемная область

Интернет-сервисы ПГИ являются результатом развития новых как коммуникационных, так и информационных технологий [2], что явилось основанием, в частности, для изменения условий лицензирования деятельности в области оказания услуг связи в стране (постановление Правительства РФ от 30.12.2020 № 2358). Интернет-сервисы расширили технологическую и функциональную возможность речевого обмена различным оконечным оборудованием пользователей услуг операторов мобильной связи, передачи данных (ПД) и телефонных сетей общего пользования (ТфОП). Исторически ТфОП и почтовая связь решили общегосударственную задачу по обеспечению связью населения и всех населенных пунктов на территории страны. Аналогичных результатов пытаются достичь операторы ПД и мобильной связи. Именно это явилось основанием для обсуждения и исследования различных сценариев (табл.) отношений между заинтересованными сторонами, которые затрагивают технические и регуляторные аспекты интернет-сервисов ПГИ в ТфОП (нормативно-правовых актов – НПА), организационные, экономические и социальные, например, междугородней (МГ), международной (МН) и местной телефонной связи (МТС) [2].

ТАБЛИЦА. Сценарии ПГИ в ТфОП

Заинтересованные стороны	Сценарий 1 (существующий)	Сценарий 2 (оптимистический) провайдер сервисов	Сценарий 3 (компромиссный) агрегатор сервисов
Мегарегулятор	Отсутствие регулирования и контроля	Лицензирование деятельности, регулирование тарифов, мониторинг и контроль трафика	Сертификация оборудования, регулирование тарифов, мониторинг и контроль ПГИ
Оператор ПД	Субъект подключения к ТфОП	Статус МГ/МН-оператор к МТС-оператору	Субъект подключения к ТфОП

Заинтересованные стороны	Сценарий 1 (существующий)	Сценарий 2 (оптимистический) провайдер сервисов	Сценарий 3 (компромиссный) агрегатор сервисов
Оператор ТфОП	Субъект подключения к ПД	МТС- оператор подключения к МГ/МН-оператору	Субъект подключения к ПД и провайдеру ПГИ
Пользователь ТфОП	Нечетко афишированная тарификация	Сбалансированная тарификация	Дотационная стоимости речевого трафика ТфОП

Результаты

Исследование регуляторных изменений интернет-сервисов ПГИ целесообразно проводить в соответствии с предлагаемой инфологической моделью (рис.).

Ограничениями при проведении исследования являются:

– существующее состояние нормативного регулирования миграции трафика интернет-сервисов ПГИ в сетях связи общего пользования;

– использование общедоступных НПА, в т. ч. в области связи;

– конфиденциальность, целостность, аутентификация пользователей и другие специальные требования по защите информации.

Основными рисками при проведении исследований являются:

– вероятность затяжного влияния состояния постковидной экономики на прогноз развития интернет-сервисов ПГИ по ТФОП;

– вероятность появления новых законодательных инициатив по проектам НПА в период проведения исследования;

– ограниченность механизмов реализации возможных способов решения проблемы;

– задачи, которые остаются нерешенными на критическом пути реализации проекта.

Методология выполнения работ базируется на проведении всестороннего анализа предмета исследования в научно-технической и практической сфере, с учетом основных влияющих факторов и условий, вскрытии противоречий, выработке обоснованных путей в современных условиях.

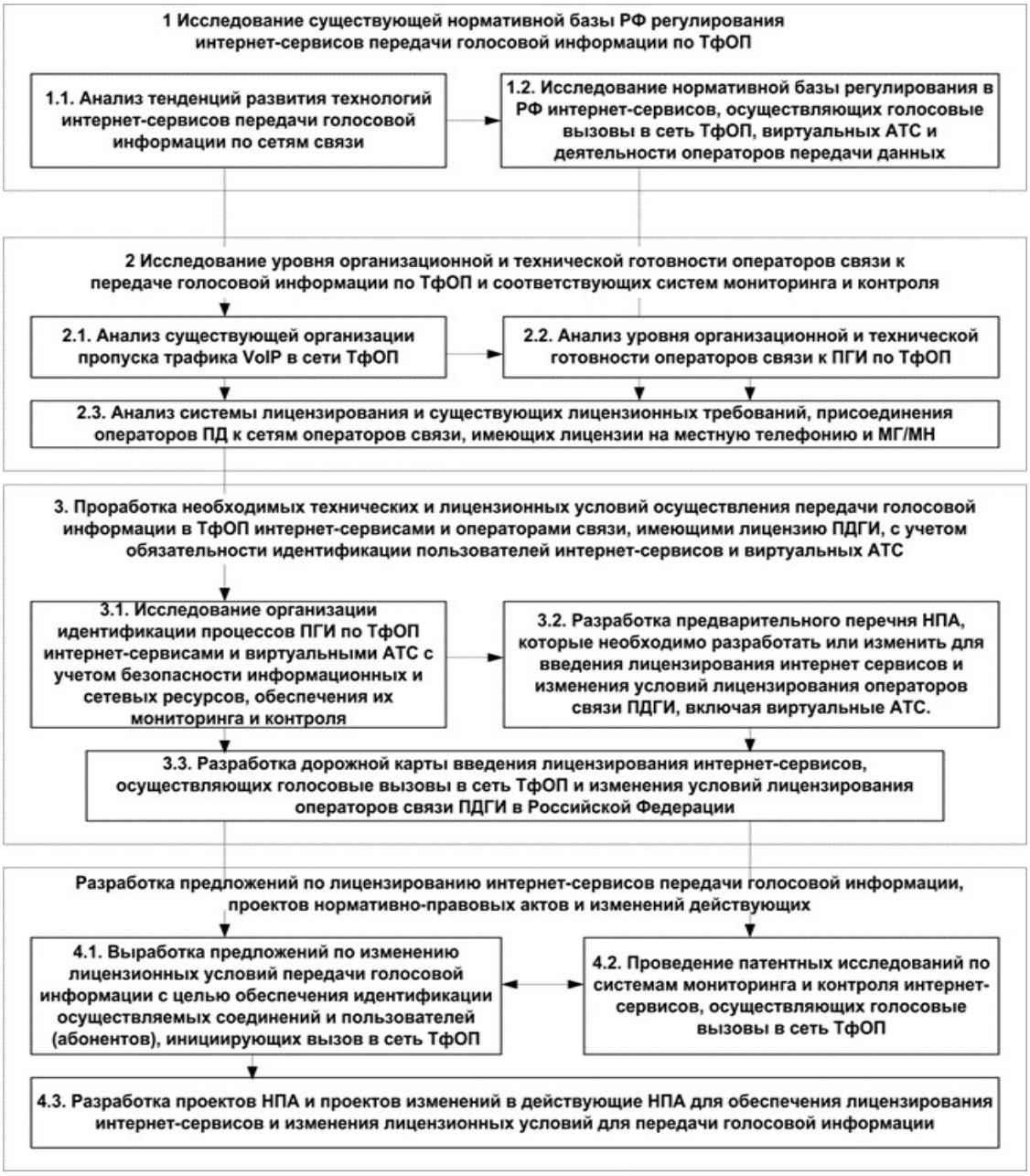


Рис. Инфологическая модель исследования

При проведении, например, анализа тенденций развития технологий интернет-сервисов ПГИ должен быть реализован системный подход с применением различных методов (экспертными, экономико-статистическими и информационными), который включает:

– анализ условий и тенденций развития технологий интернет-сервисов передачи информации, в том числе ПГИ;

– исследование сегмента рынка интернет-сервисов ПГИ;

– разработку (уточнение) классификации интернет-сервисов ПГИ, принципов их организации и реализации на ССОП.

При выработке предложений по лицензированию интернет-сервисов, осуществляющих голосовые вызовы в сеть ТфОП, целесообразно применять системный подход и комплексные исследования проблем, которые возникают в рамках оказания услуг связи в гетерогенных сетях и различных правовых отношений субъектов взаимодействия, их организационной и технической обеспеченности.

Основными методами в процессе всего исследования целесообразно принять:

– методы (процедуры) мониторинга правоприменения;
– методы научно-технического прогнозирования, моделирования знаний для изучения характера развития технологии;
– методы анализа тенденций и др.;
– методы информационного анализа, статистического анализа;
– методы фактографического анализа;
– методы дискретно-непрерывной математики;
– методы теории систем, систем и сетей массового обслуживания;
– методы теории риск-менеджмента.

Дорожная карта регуляторных изменений для исследуемой проблемной области включает: процедуры разработки концепции проектов НПА, процедуры согласования проектов НПА и изменения в действующие НПА в части лицензирования интернет-сервисов и лицензионных условий для ПГИ по ТфОП.

Заключение

Регуляторные изменения интернет-сервисов ПГИ являются объективным следствием развития современных цифровых сквозных технологий, изучение которых целесообразно проводить в рамках формируемой программы комплексных междисциплинарных исследований по тематике технологий интернет-сервисов и правовых основ цифровой экономики организации передачи голосовой информации в гетерогенных коммуникациях. Рассмотренные методологические подходы целесообразно использовать в качестве основы междисциплинарных исследований.

Список используемых источников

1. Бачевский С. В., Шестаков А. В. Связь-2030: Стратегии технологического совершенствования и регуляторных изменений // "Цифровая экономика. Новое время – новые технологии. Росинфоком 2020" Росинфоком-2020. Материалы VI Всероссийской научно-технической конференции (г. Самара, 18 ноября 2020 г.). Самара: ПГУТИ, 2020. С. 11–12.

2. Граф связности AS по странам по данным RIR. URL: https://www.ididb.ru/connectivity.

УДК 004.9
ГРНТИ 81.93.29

ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К ОРГАНИЗАЦИЯМ ДЛЯ ПРОТИВОДЕЙСТВИЯ АТАКАМ НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ МЕТОДАМИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

А. Ю. Ярошенко

Департамент информационных технологий и связи МЧС России

В статье рассматривается задача противодействия социальным атакам, направленным на информационные ресурсы организации. При этом атакуемым объектом является сотрудник организации, а атакующим – нарушитель, зачастую опосредованно через программно-аппаратные средства. Для этого рассматриваются 4 наиболее распространённых сценария таких атак: звонок из банка, поддельное почтовое письмо, «забытый» зараженный носитель данных и психоэмоциональное воздействие на человека. На основании сценариев предлагаются различные подходы для противодействия атакам, направленные на элементы последних: легального пользователя, нарушителя и само воздействие. Как результат, формируются девять обобщенных требований к организациям (по 3 к каждому элементу атаки), направленным на противодействие социальным атакам.

информационная безопасность, информационный ресурс, социальная атака, противодействие, требования к организации.

Введение

Стремительное развитие информатизации, привнесшее в современную жизнь множество положительных факторов [1], также стало причиной появления нового вида угроз – информационных [2]. И если в начале развития сферы информационной безопасности их источниками считались в основном программно-аппаратные средства, то теперь лидирующее положение зачастую занимает человеческий фактор, успешно используемый в социальной инженерии – т. е. в данном случае при проведении социальных атак на информационные ресурсы. Как следствие, возникает потребность расширения требований к организациям по противодействию атакам, проводимым методами социальной инженерии [3].

Распространенные сценарии атак

К наиболее известным (в негативном смысле) сценариям социальных атак можно отнести следующие. Во-первых, это звонок от имени сотрудника банка с сообщением о подозрительной транзакции и запросом персональных данных владельца счета [4]. Полученная информация может быть использована злоумышленником для проведения последующих атак (в т. ч. социальных). Самым критичным, естественно, будет ситуация, если пользователь сообщит свой логин и пароль для доступа в личный кабинет или PIN-код банковской карты (или данные для доступа к личному кабинету организации в банке). Во-вторых, популярным сценарием атак является рассылка почтовых писем с письмом, маскируемым под сообщение от банка. При этом домен адреса отправителя внешне похож на домен реального банка, однако не является им (например, поддельный *s6er6ank.ru* подлинного *sberbank.ru*). Естественно, пользователь может отреагировать на это письмо, как если бы оно было настоящим – перейти по ссылке (ведущей на подставной сайт, запрашивающий логин и пароль пользователя, при этом внешне полностью совпадающий с сайтом банка). Как результат, аналогично первому сценарию, данные пользователя будут похищены [4]. В-третьих, атаки по так называемому сценарию «дорожного яблока», когда в организации разбрасываются (в прямом смысле) носители данных (USB-накопители, флеш-карты, CD/DVD диски и пр.) с притягательным названием (например, «фото с отдыха», «финансовый отчет», «секреты»), которое будет играть на людском любопытстве [5]. Обнаружив такой бесхозный носитель (содержащий программы с вредоносным кодом [6-9]), пользователь может ее вставить в рабочий компьютер на территории организации (т. е., по сути, стать невольным инсайдером [10]), что с некоторой вероятностью приведет к заражению всей сети организации [11]. Четвертым сценарием, также крайне популярным и действенным, можно считать любые воздействия на психоэмоциональное состояние человека с целью получения от него необходимой информации [12]: угрозы, уговоры, взывание к жалости, подкуп (используя жадность) и пр.

Подходы к противодействию атакам

Противодействие социальным атакам является достаточно сложным процессом, поскольку он крайне сложно формализуем. Причина этого заключается именно в особенностях трех составляющих атаки: легальный пользователь, нарушитель, методы воздействия. Все эти элементы отличает одна особенность – наличие человеческого фактора, создание для которого математических аппаратов еще до сих пор является нерешенной проблемой. Тем не менее можно предположить следующие подходы, направленные на составляющие. Во-первых, необходимо обучать легальных пользовате-

лей самим защищаться от подобного рода атак – путем привлечения в различные обучающие программы, создания игровых ситуаций с участием пользователей и симулированием атак (с последующим разъяснением допущенных ошибок), общего повышения компьютерной грамотности среди далекого от области IT-персонала. Во-вторых, необходимо противодействовать и нарушителям, применяющим методы социальной инженерии для атаки на информационные ресурсы [13]. Возможно, имеет смысл дополнить законодательную базу учетом подобных нарушений; что, однако, однозначно будет сложной юридической задачей. И, в-третьих, можно противодействовать самим методам воздействия – например, огородив от них сотрудников организации (повышая мотивацию честного выполнения должностных обязанностей, объясняя почетность и престиж работы в организации, отслеживая и пресекая подозрительные и опасные контакты между сотрудниками или с внешними организациями). Также, как в случае сценария с «дорожным яблоком», даже банальный контроль за посторонними предметами может дать свои плоды для успешного противодействия – банальный сбор информации о неприметных на первый взгляд инцидентах (обнаружение на веб-камерах нескольких потерянных USB-накопителей за короткий промежуток времени, болезнь администратора сети после неожиданного приема на работу его заместителя, детектирование повышенной активности спам-рассылок сотрудникам некоторого отдела) после анализа (экспертами по информационной безопасности или с привлечением искусственного интеллекта) может стать сигналом о целенаправленной социально-инженерной атаки на организацию. Также, очевидно, что для лучшего результата такие подходы необходимо применять комплексно [14, 15].

Обобщенные требования к организациям

Исходя из озвученных подходов к защите информационных ресурсов от социальных атак можно предложить следующие 9 обобщенных требований к организациям (по три, направленных на каждый элемент) [16, 17].

Для легального пользователя:

1) Тестирование и выявление сотрудников при приеме на работу на предмет уязвимости к социальным атакам;

2) Проведение тренингов и прочих мероприятий по обучению сотрудников выявлению социальных атак и противодействия им;

3) Формирование и учет требований по недопущению проведения социальных атак при проектировании, разработке или закупке программно-аппаратных средств для использования в организации.

Против нарушителя:

4) Тестирование и выявление сотрудников при приеме на работу на предмет заинтересованности и возможности проведения социальных атак;

5) Регламентирование, контроль и пресечение поведения посетителей организации (гостей, клиентов, заказчиков, персонала привлекаемых служб и т. п.) в части применения ими социальных приемов влияния на сотрудников;

6) Использование отдельных «шлюзов» для контактирования с ключевыми сотрудниками организации в виде подготовленных специалистов с навыками противодействия социальным атакам;

Против атакующего воздействия:

7) Систематизация и контроль социальных связей внутри организации и с внешними сотрудниками, организациями;

8) Учет в базе инцидентов информационной безопасности организации подозрительных информационных объектов и процессов, относящихся к типовым социальным атакам (обнаруженные USB-накопители, аномалии в социальном поведении и т. п.);

9) Пресечение раскрытием информации, которая может быть использована нарушителем для социальных манипуляций (личная жизнь, увлечения, слабые стороны, особенности характера и т. п.); для организаций с повышенным уровнем критичности нарушения безопасности – запрет опубликования личностной информации сотрудников в социальных сетях; а в случае невозможности скрытие информации – легендирование данных о сотрудниках.

Заключение

В ходе исследования на основании распространённых социальных атак были выделены их общие особенности и произведена их систематизация. В результаты были предложены походы по противодействию атакам, направленным на различные объекты такого воздействия. Анализ же последних позволил сформировать набор обобщенных требований к организациям, даже частичное следование которым позволит существенно снизить реализацию угроз к информационным ресурсам организации.

Список используемых источников

1. Антюхов В. И., Остудин Н. В., Ярошенко А. Ю., Черных А. К. Информационная потребность должностных лиц центров управления в кризисных ситуациях (ЦУКС) МЧС России // Сервис безопасности в России: опыт, проблемы, перспективы. Обеспечение безопасности при чрезвычайных ситуациях: сборник трудов VII Международной научно-практической конференции (Санкт-Петербург, 2015). 2015. С. 70–71.

2. Антюхов В. И., Сугак В. П., Ярошенко А. Ю., Остудин Н. В. Моделирование процесса обеспечения безопасности информации в подразделениях МЧС России // Сервис безопасности в России: опыт, проблемы, перспективы. Обеспечение безопасности при чрезвычайных ситуациях: сборник трудов VII Международной научно-практической конференции (Санкт-Петербург, 2015). 2015. С. 71.

3. Кузнецов М., Симдянов И. Социальная инженерия и социальные хакеры. СПб. : БХВ-Петербург, 2007. 368 с.

4. Деренко Н. В. Роль технологий социальной инженерии в киберпреступности // Трансформация социального мира в современную эпоху: сборник научных трудов. 2019. С. 147–151.

5. Полозюк А. Г., Коняхина С. С. Социальная инженерия – угроза информационной безопасности // Приоритетные научные направления: от теории к практике. 2016. № 29. С. 68–72.

6. Израилов К. Е. Алгоритмизация машинного кода телекоммуникационных устройств как стратегическое средство обеспечения информационной безопасности // Национальная безопасность и стратегическое планирование. 2013. № 2 (2). С. 28–36.

7. Буйневич М. В., Израилов К. Е. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 1. Функциональная архитектура // Информационные технологии и телекоммуникации. 2016. Т. 4. № 1. С. 115–130.

8. Израилов К. Е. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 2. Информационная архитектура // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 86–104.

9. Израилов К. Е., Покусов В. В. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 3. Модульно-алгоритмическая архитектура // Информационные технологии и телекоммуникации. 2016. Т. 4. № 4. С. 104–121.

10. Буйневич М. В., Власов Д. С. Аналитический обзор моделей инсайдеров информационных систем // Информатизация и связь. 2020. № 6. С. 92–98.

11. Ярошенко А. Ю. Системный подход к внедрению и настройке межсетевых экранов в государственных информационных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании: V международная научно-техническая и научно-методическая конференции: сб. науч. ст. СПб. : СПбГУТ, 2016. С. 551–554.

12. Анацкая А. Г., Долгих Е. С. Социальная инженерия в аспекте информационной безопасности // Архитектурно-строительный и дорожно-транспортный комплексы: проблемы, перспективы, новации: материалы Международной научно-практической конференции. Омск, 2016. С. 860–864.

13. Буйневич М. В., Власов Д. С. Сравнительный обзор способов выявления инсайдеров в информационных системах // Информатизация и связь. 2019. № 2. С. 83–91.

14. Ярошенко А. Ю., Буйневич М. В. Обоснование потребности в методике оценки качества и эффективности комплексной организационно-технической системы обеспечения безопасности информации в МЧС России // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2016. № 4. С. 57–62.

15. Буйневич М. В., Покусов В. В., Ярошенко А. Ю., Хорошенко С. В. Категориальный подход в приложении к синтезу архитектуры интегрированной системы обеспечения безопасности информации // Проблемы управления рисками в техносфере. 2017. № 4 (44). С. 95–102.

16. Алейникова О. В., Базарова А. А., Цап Т. В. Требования безопасности объектов критической информационной инфраструктуры и этапы их реализации // Информационные технологии и системы: управление, экономика, транспорт, право. 2019. № 3 (35). С. 70–76.

17. Добродеев А. Ю. Показатели информационной безопасности как характеристика (мера) соответствия сетей и организаций связи требованиям информационной безопасности // Труды ЦНИИС. Санкт-Петербургский филиал. 2020. Т. 2. № 10. С. 50–78.

Статья представлена доцентом кафедры ЗСС СПбГУТ кандидатом технических наук К. Е. Израиловым.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РАДИОЭЛЕКТРОНИКИ И СИСТЕМ СВЯЗИ

УДК 621.373.5
ГРНТИ 47.45.33

МИКРОВОЛНОВЫЙ ГЕНЕРАТОР НА ПОЛУСФЕРЕ

Е. И. Бочаров, Е. А. Коновалова, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе исследована возможность генерации сигнала при помещении активного двухполюсника в резонатор, в качестве объёмного резонатора используется полусфера. Для детального исследования данного устройства создан проволочный эквивалент полусферы. Разработаны и описаны компоненты генератора и экспериментальная установка генератора на активном двухполюснике. Исследовано наличие генерации в зависимости от места установки двухполюсника и места съема энергии. Доказана работоспособность предложенной модели.

СВЧ, сферический резонатор, генератор СВЧ.

Эквивалентом полусферического резонатора является проволочная модель [1, 2]. Макет предлагаемого эквивалента представляет собой распределенную ёмкость каждого проводника на землю и непосредственно индуктивность каждого проводника (рис. 1). На рис. 2 (см. ниже) представлены проволочный эквивалент и АЧХ полусферического резонатора.

Простейшая формула для расчета добротности резонатора [3, 4]:

$$Q = \frac{V}{S \cdot d},$$

где V – объём резонатора,

S – площадь поверхности резонатора,

d – толщина скин-слоя. Толщина скин-слоя для меди на частоте порядка 10^9 Гц составляет 2,09 мкм.

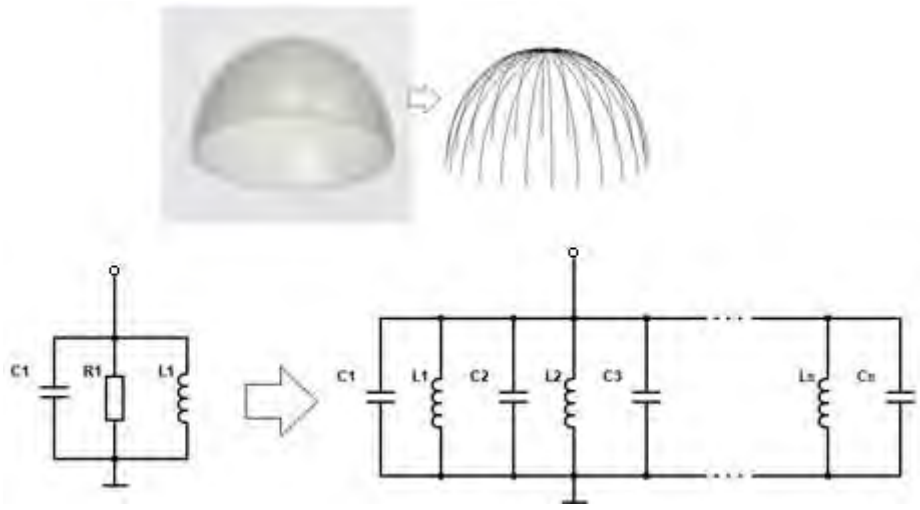


Рис. 1. Эквивалент полусферического резонатора и его принципиальная схема

Для сферического резонатора:

$$V_1 = \frac{4}{3}\pi R^3 = \frac{4 \cdot 3{,}14 \cdot (0{,}044\ \text{м})^3}{3} = 3{,}568 \cdot 10^{-4}\ \text{м}^3,$$

$$S_1 = 4\pi R^2 = 4 \cdot 3{,}14 \cdot (0{,}044\ \text{м})^2 = 0{,}024\ \text{м}^2,$$

$$Q_1 = \frac{R}{3d} = \frac{0{,}044\ \text{м}}{3 \cdot 2{,}09 \cdot 10^{-6}\ \text{м}} = 7018.$$

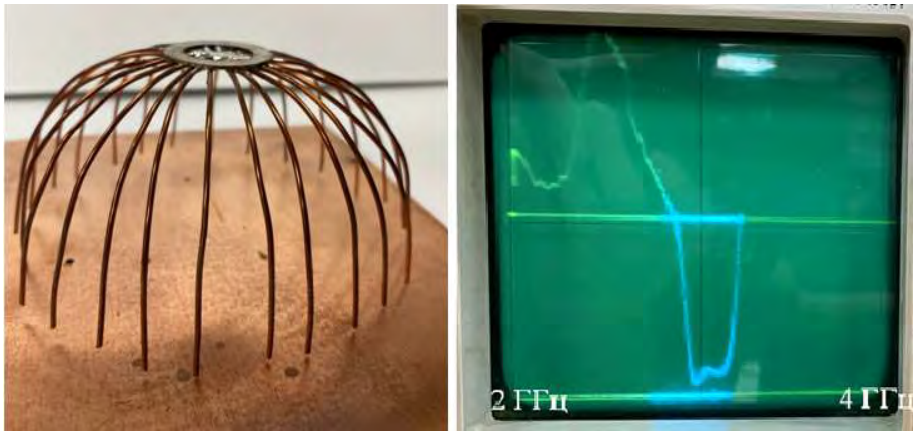


Рис. 2. Проволочный эквивалент и АЧХ полусферического резонатора

Для полусферического резонатора:

$$V_2 = \frac{2}{3}\pi R^3 = \frac{2 \cdot 3{,}14 \cdot (0{,}044\ \text{м})^3}{3} = 1{,}784 \cdot 10^{-4}\ \text{м}^3,$$

$$S_2 = 3\pi R^2 = 3 \cdot 3{,}14 \cdot (0{,}044\ \text{м})^2 = 0{,}018\ \text{м}^2,$$

$$Q_2 = \frac{2R}{9d} = \frac{2 \cdot 0{,}044 \text{ м}}{9 \cdot 2{,}09 \cdot 10^{-6} \text{ м}} = 4678.$$

Таким образом, добротность полусферы составляет 2/3 добротности сферы.

Была предложена модель установки активного двухполюсника с отрицательным сопротивлением в один из проводников. Предложенная модель и её принципиальная схема выглядит следующим образом (рис. 3).

Также был изготовлен макет предлагаемого устройства (рис. 4) и произведена проверка работоспособности.

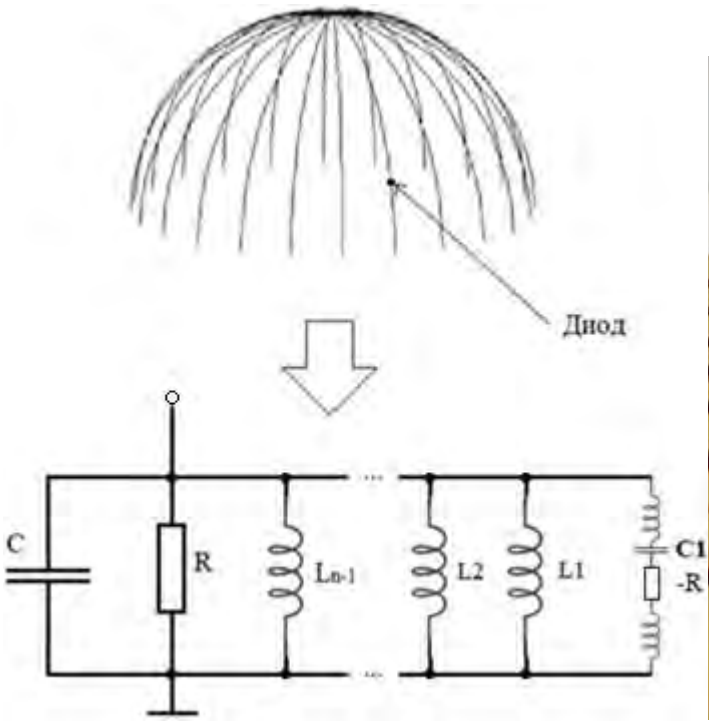


Рис. 3. 3D модель и принципиальная схема генератора

Рис. 4. Макет генератора

В ходе проверки на работоспособность предложенного полусферического устройства генерации с активным двухполюсником была получена генерация в диапазоне до 500 МГц.

В дальнейшем активный двухполюсник был установлен во внутреннем объёме масштабного макета полусферического резонатора (рис. 5), в этом случае получена генерация в точном соответствии с частотной характеристикой объёма.

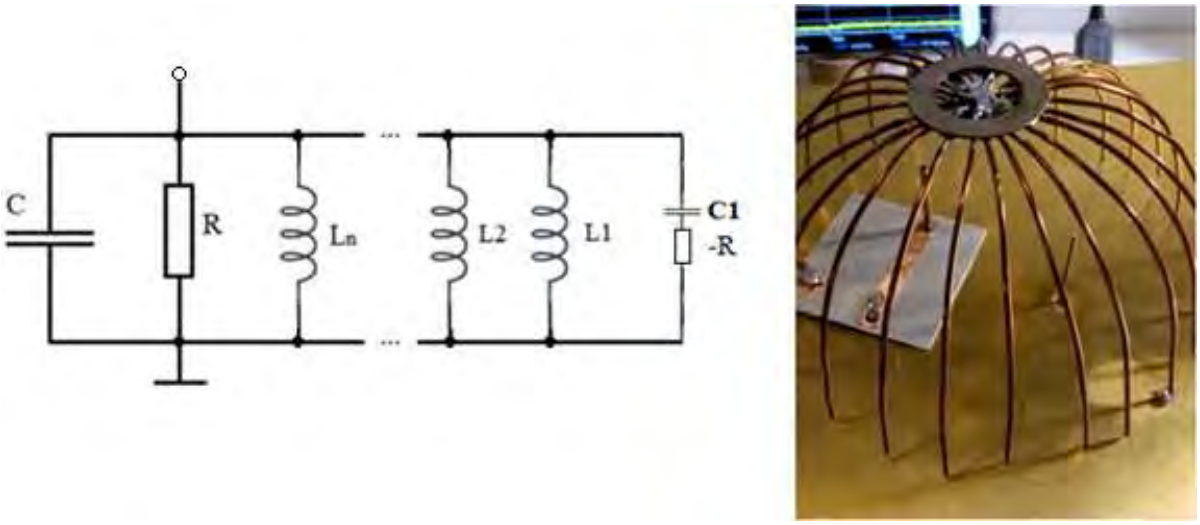


Рис. 5. Принципиальная схема и рабочий макет генератора

Рабочими являются частоты 2,890 и 3,135 ГГц, которые соответствует двум наилучшим КСВН частотной характеристики резонатора. Из спектрограммы (рис. 6) видно, что полусферический эквивалент резонатора является хорошим устройством повышения стабильности частоты колебания. Основное колебание превышает побочные на 40 дБ.

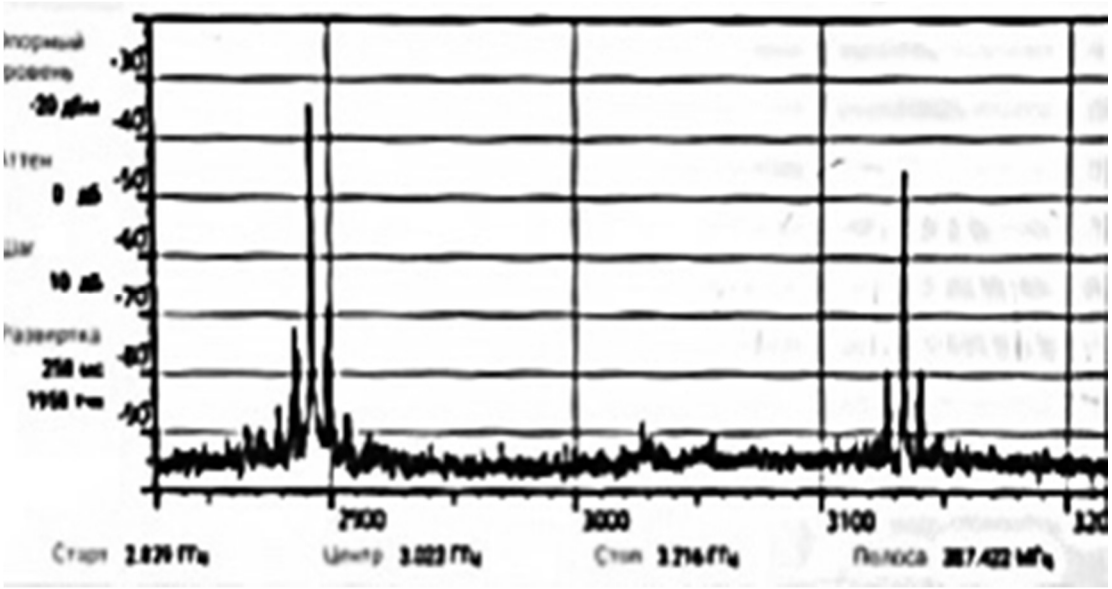


Рис. 6. Спектральная характеристика генератора

Вывод: исследования показали, что полусферический резонатор может быть использован при создании высокостабильных генераторов СВЧ диапазона. Не вызывает сомнений, что его эквивалент в виде проволочной модели, рассчитанной на заданные частоты также способен повышать стабильность частоты колебания в заданном диапазоне.

Доказана работоспособность микроволнового генератора на полусфере.

Список используемых источников

1. Бочаров Е. И., Коновалова Е. А., Седышев Э. Ю. Исследование проволочной модели полусферы в качестве резонатора СВЧ // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2020). Региональная научно-методическая конференция магистрантов и их руководителей: сб. лучших докладов конф. / Сост. Н. Н. Иванов. СПб.: СПбГУТ, 2021. С. 322–325.

2. Бочаров Е. И., Коновалова Е. А., Седышев Э. Ю. Исследование генератора на активном двухполюснике в сферическом резонаторе // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2020. С. 401–403.

3. Каценеленбаум Б. З. Высокочастотная электродинамика: Основы математического аппарата. М. : Наука, 1966. 240 с.

4. Фальковский О. И. Техническая электродинамика. М.: Связь, 1978. 431 с.

УДК 621.375.4
ГРНТИ 47.43.33

СВЧ-УСИЛИТЕЛЬ НА ГИБРИДНОМ КОЛЬЦЕ С АКТИВНЫМИ ДВУХПОЛЮСНИКАМИ

Е. И. Бочаров, М. О. Подольская, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа посвящена синтезу малошумящего усилителя СВЧ. Предметом исследования является гибридный мост на микрополосковой линии и включенные в его плечи активные двухполюсники. На основе гибридного кольца сумматора создается усилитель СВЧ диапазона. В ходе работы был создан макет устройства на активных двухполюсниках, включенных в гибридный кольцевой мост при помощи шлейфов. Проведена компьютерная эмуляция работоспособности устройства и экспериментальные исследования.

СВЧ, направленный ответвитель, микрополосковая линия, усилитель, усилительный диод.

Мостовые устройства интересны для разработчиков возможностью получения высокой точности синфазно-противофазного деления мощности СВЧ сигнала, а также простотой конструктивного выполнения. Кольцевые мосты (КМ) выполняются на симметричных (СПЛ) или несимметричных (НПЛ) полосковых линиях, свёрнутых в кольцо с длинной равной 3λ/2.

По эквивалентной схеме КМ видно, что плечи включены симметрично на расстоянии λ/4 друг от друга, одна из секций кольца имеет длину 3λ/4 (рис. 1) [1].

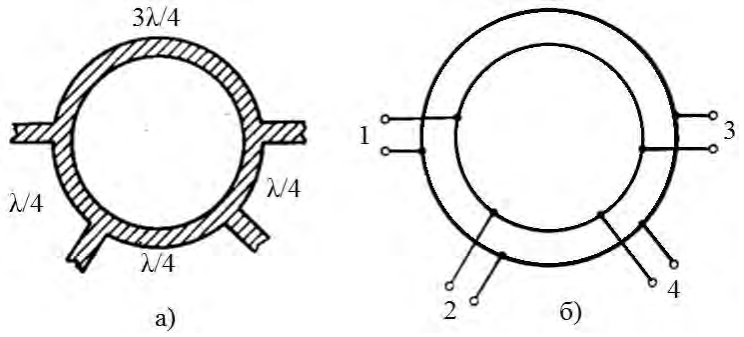


Рис. 1. Кольцевой мост с периметром 3λ/2 (а), эквивалентная схема (б)

Волновая матрица рассеяния данного КМ с учетом потерь в линии передачи выглядит следующим образом:

$$S_{11} = \frac{\alpha l Y_2^2}{p},\ S_{12} = -\frac{iY_1[\alpha l(3Y_1 + Y_2) + 1]}{p},$$

$$S_{21} = -\frac{iY_2[\alpha l(2Y_1 + Y_2) + 1]}{p},\qquad S_{22} = \frac{-\alpha l Y_1^2 Y_2}{p},$$

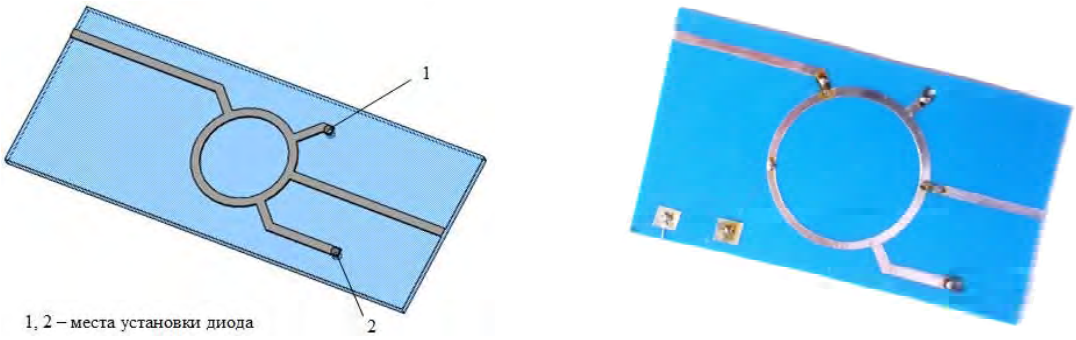
где $\alpha = \frac{52{,}17\pi c}{Q_0\sqrt{\varepsilon}}$ – потери в линии передачи (c – скорость света, Q_0 – добротность линии передачи),

l – периметр КМ,

$Y_{1(2)}$ – волновые проводимости линий, $p = 2\alpha l(2Y_1 + Y_2) + 1$ [1].

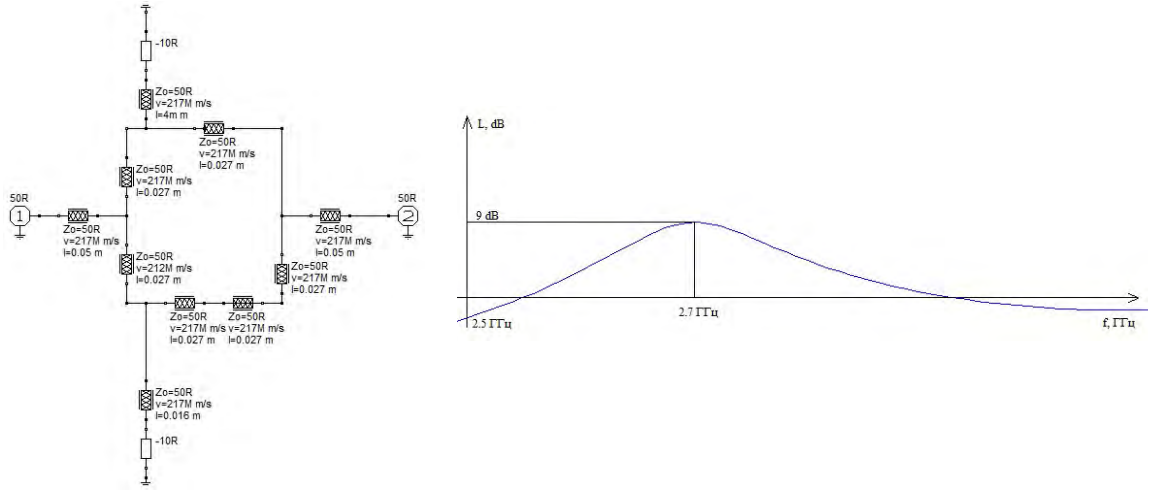
На основе КМ разработан СВЧ усилитель, путём включения в шлейфы кольца активных двухполюсников (диодов) [2]. Входная и выходная цепи усилителя разделяются с помощью 2-х диодов, работающих на отражение и связанных гибридным соединением. Мощность сигнала, поступающего в гибридное кольцо, делится пополам и подводится к двухполюсникам. Отраженные от них сигналы в цепи нагрузки складываются (рис. 2).

В пакете RFSimm99 была разработана эквивалентная схема устройства и произведена эмуляция его работы, расчётная частота усилителя 2 ГГц. В качестве эквивалента активным двухполюсникам используются резисторы с отрицательным сопротивлением (рис. 3).



а) б)

Рис. 2. Модель (а) и макет (б) усилителя СВЧ на гибридном кольце



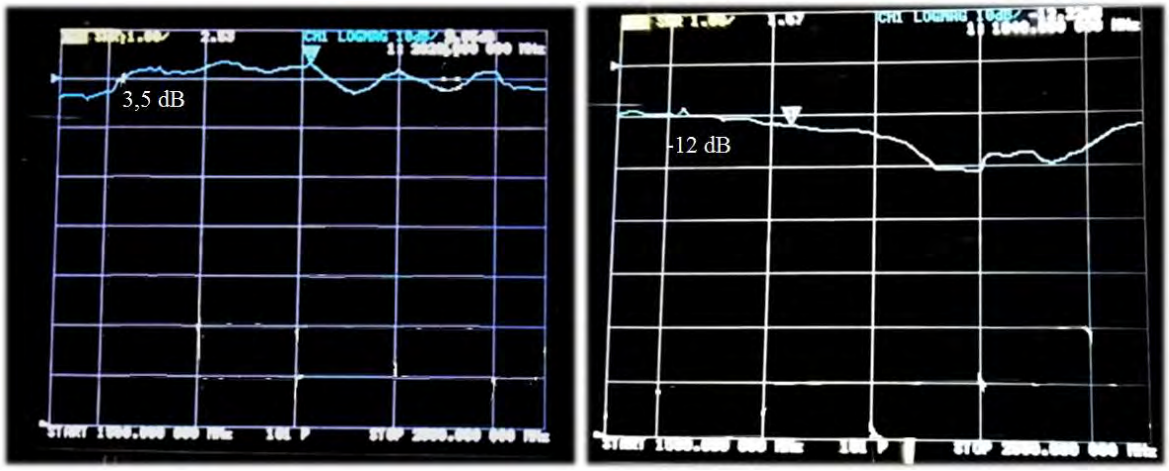
а) б)

Рис. 3. Эквивалентная схема усилителя (а); АЧХ усилителя на КМ (б)

Из графика на рис. 2 (б) видно, что на частоте 2,7 ГГц наблюдается усиление порядка 9 дБ.

Далее макет был исследован. На графике рис. 4 (а) показана АЧХ кольцевого моста без включения питания диодов, на нём наблюдается ослабление 12 dB на частотах 1,6–1,8 ГГц. При подаче питания на диоды график изменяется, и на тех же частотах усиление составляет порядка 3,5 – 4 дБ, различие результатов компьютерного моделирования и измерения макета усилителя связано с тем, что он рассогласован.

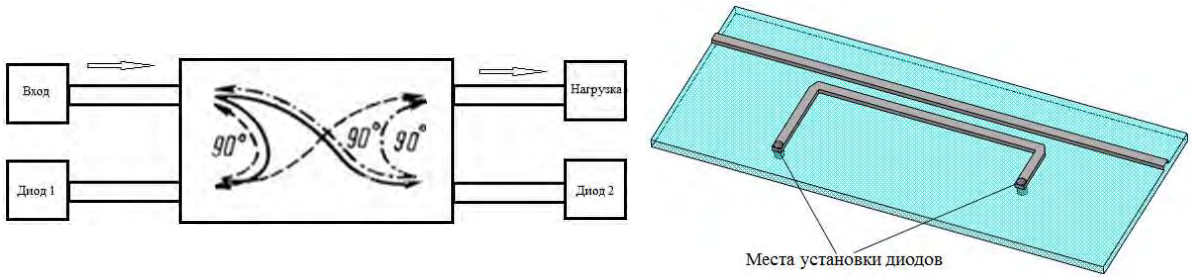
Результат исследования устройства доказывает возможность использования мостовых схем с двумя диодами. Что возвращает нас к работе над усилителем на направленном ответвителе (НО) с включением двух диодов [2].



а) б)

Рис. 4. АЧХ усилителя без подачи питания на диоды (а); с питанием диодов (б)

Существуют гибридные соединения, работающие в широком диапазоне частот. Такие соединения представляют собой две связанные линии. В нашем случае – это направленный ответвитель с установленными в его плечи двумя активными двухполюсниками. В такой системе так же осуществляется направленное распространение сигнала (рис. 5).

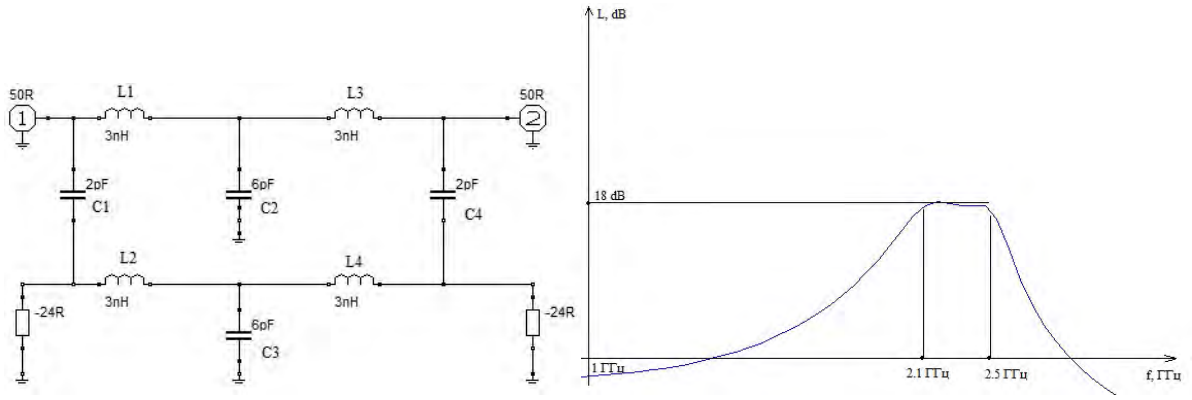


а) б)

Рис. 5. Схема распространения сигнала в устройстве (а)
и модель усилителя на НО (б)

В качестве примера была произведена эмуляция схемы, приведенной на рис. 6 (а) [3] усилителя на НО в пакете RFSimm99. Она показала, что в диапазоне 2,1…2,5 ГГц (полоса пропускания 400 МГц) наблюдается усиление порядка 18 дБ.

Данный вариант исполнения усилителя СВЧ можно считать наиболее перспективным, для его физической реализации требуется точное матричное описание НО (с помощью S-параметров) в заданном диапазоне частот. Возможность использования мостовых схем в качестве усилителей полностью доказана работоспособностью гибридных колец.



а) б)

Рис. 6. Эквивалентная схема усилителя на НО (а);
АЧХ усилителя в заданном диапазоне частот (б)

Список используемых источников

1. Гвоздев В. И., Нефёдов Е. И. Объемные интегральные схемы СВЧ. М.: Наука. Главная редакция физико-математической литературы, 1985. 256 с.

2. Бочаров Е. И., Подольская М. О., Седышев Э. Ю. Синтез усилителя СВЧ с использованием схем деления мощности // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2020). Региональная научно-методическая конференция магистрантов и их руководителей: материалы конференции. СПб.: СПбГУТ, 2020. С. 803–805.

3. Аксенов А. Е. Направленный ответвитель на сосредоточенных индуктивных и емкостных элементах // Радиотехника. 1976. № 2.

УДК 621.373
ГРНТИ 47.41.31

ПРОЕКТИРОВАНИЕ ПРЕСЕЛЕКТОРА ИЗМЕРИТЕЛЬНОГО ПРИЁМНИКА

Е. А. Брусин[1], П. И. Елгин[2], М. В. Коршунов[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Филиал ФГУП НИИР – ЛОНИИР

При построении измерительных приёмников аппаратуры измерения параметров радиопомех возникает необходимость разработки схем предварительной частотной селекции сигналов. Основной проблемой при создании преселектора является разработка усилительных схем, предназначенных компенсация потерь фильтрах и коммутаторах, включённых в тракт. Рассмотрено построения преселектора с использованием

схем малошумящих усилителей на основе СВЧ арсенид-галлиевых полевых транзисторов отечественного производства.

электромагнитная совместимость, полосы измерительных приёмников, СВЧ арсенид-галлиевый полевой транзистор, малошумящий усилитель.

Постановка задачи

В настоящее время используются полосы частот приёмников-измерителей помех в диапазоне от 9 кГц до 18 ГГц [1, 2]. В структуру тракта приёмника входит схема преселектора [3], в функции которого входит обеспечение частотной селекции сигнала. В полосе 1…18 ГГц в качестве преселектора могут использоваться схемы на основе перестраиваемых фильтров на ЖИГ-резонаторах [4, 5, 6]. К недостаткам этих фильтров следует отнести высокую стоимость и значительное энергопотребление. Поэтому представляется целесообразным рассмотреть подход на основе набора полосовых фильтров и коммутаторов [5]. Структура такого преселектора в полосе 1…16 ГГц представлена на рис. 1. Полосовые фильтры реализованы на основе стандартных фильтров верхних и низких частот (ФВЧ и ФНЧ) [7]. Для компенсации потерь в фильтрах и шумов коммутатора в схему включены усилители. Задача усилителя компенсировать собственные потери коммутатора. Так, например, максимальные потери коммутатора HMC641 фирмы Analog Devices не превосходят 2,4 дБ [8]. Таким образом, достаточен усилитель с усилением около 6 дБ. Представляется целесообразным реализовать данные усилители на основе однокаскадных транзисторных малошумящих усилителей (МШУ), специально предназначенных для использования в сочетании с коммутатором, представленном на рис. 1. Практический интерес имеет разработка усилителей на отечественных транзисторах. В связи с этим, при проектировании была поставлена задача разработки линейки усилителей в диапазоне частот от 1 до 16 ГГц на отечественных транзисторах и схемы преселектора на основе этих усилителей.

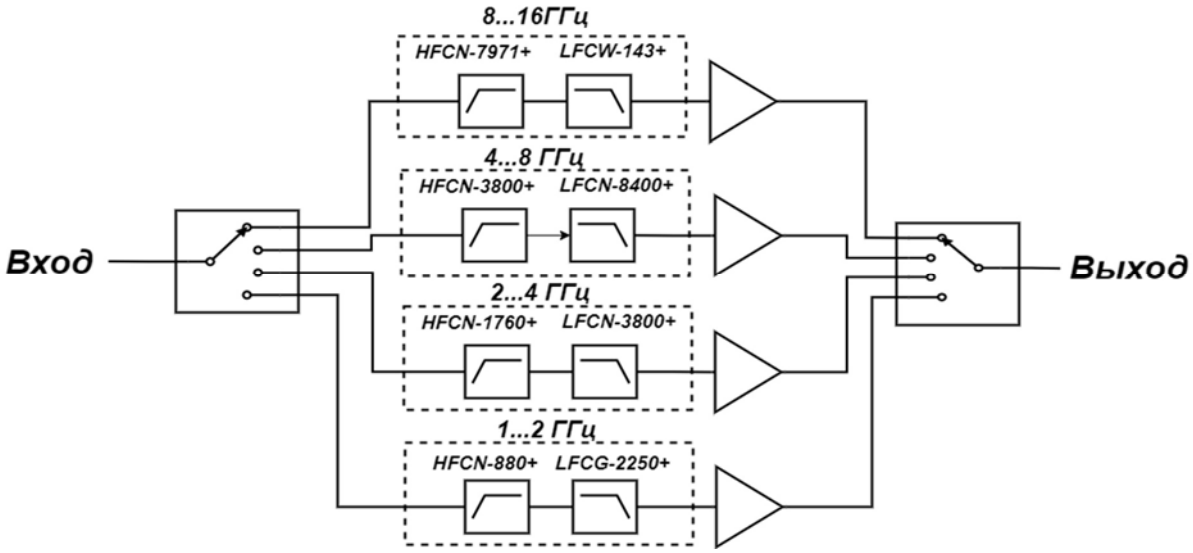


Рис. 1. Структура преселектора в полосе 1…16 ГГц

Разработка усилителей

В качестве активного элемента в современных схемах МШУ используются как биполярные, так и полевые транзисторы [9, 10]. Что касается отечественной элементной базы, то в плане построения схем усилителей в диапазоне 1…16 ГГц практически нет альтернативы арсенид-галлиевым транзисторам производства ЗАО «НПП «Планета-Аргалл» [11].

Усилитель на диапазон 1…2 ГГц может быть реализован на основе транзисторов серии 3П373. S-параметры транзисторов в полосе 1…8 ГГц представлены в таблице. Параметры, описанные в таблице, позволяют создать модель транзистора для САПР AWR microwave office.

Схема предлагаемого усилителя показана на рис. 2, топология усилителя на рис. 3. Параметры усилителя иллюстрируют зависимости, представленные на рис. 4. Схема более высокочастотной части тракта реализована на основе транзисторов 3П374 и 3П385. Структура преселектора представлена на рис. 5.

Преселектор включает в себя два ключа на два направления (SPDT), ветвь 9 кГц…1 ГГц и схема преселектора, построенная на основе МШУ, разработанных на базе транзисторов 3П373, 3П374 и 3П375.

ТАБЛИЦА. S-параметры транзисторов 3П373А,Б,В

Частота f, ГГц	S_{11}		S_{21}		S_{12}		S_{22}	
	М(дБ)	φ(град)	М(дБ)	φ(град)	М(дБ)	φ(град)	М(дБ)	φ(град)
0.5	0.9911	-18.5845	5.5308	166.8671	0.0284	78.9917	0.5119	-13.8621
1.0	0.9671	-36.4208	5.2944	154.3208	0.0542	68.5704	0.4945	-27.1196
1.5	0.9340	-52.9650	4.9601	142.7660	0.0761	59.1415	0.4705	-39.3502
2.0	0.8982	-67.9537	4.5835	132.3657	0.0935	50.8684	0.4440	-50.3757
2.5	0.8640	-81.3537	4.2060	123.0954	0.1069	43.7274	0.4184	-60.2079
3.0	0.8338	-93.2687	3.8512	114.8319	0.1170	37.5955	0.3954	-68.9605
3.5	0.8081	-103.8623	3.5294	107.4209	0.1245	32.3191	0.3757	-76.7812
4.0	0.7869	-113.3106	3.2430	100.7137	0.1300	27.7503	0.3595	-83.8152
4.5	0.7698	-121.7797	2.9903	94.5819	0.1341	23.7615	0.3464	-90.1901
5.0	0.7561	-129.4162	2.7679	88.9203	0.1370	20.2481	0.3362	-96.0128
5.5	0.7452	-136.3454	2.5721	83.6443	0.1390	17.1266	0.3286	-101.3713
6.0	0.7367	-142.6726	2.3993	78.6873	0.1404	14.3313	0.3231	-106.3370
6.5	0.7302	-148.4854	2.2461	73.9963	0.1412	11.8103	0.3196	-110.9687
7.0	0.7253	-153.8567	2.1097	69.5297	0.1416	9.5230	0.3177	-115.3145
7.5	0.7218	-158.8468	1.9877	65.2541	0.1416	7.4375	0.3173	-119.4142
8.0	0.7194	-163.5058	1.8781	61.1429	0.1414	5.5285	0.3181	-123.3011

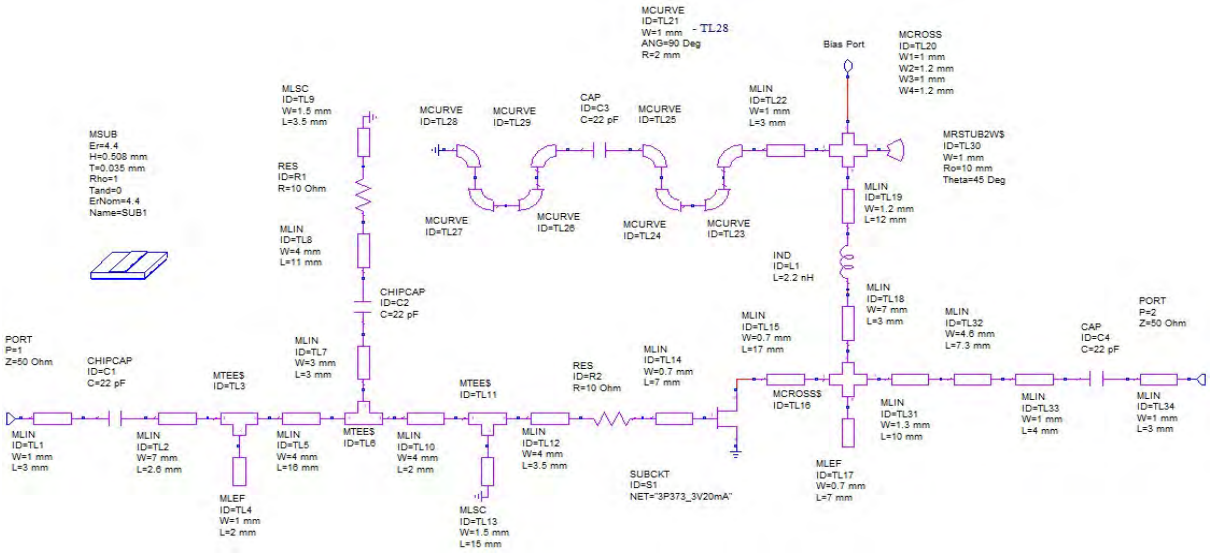


Рис. 2. Схема усилителя полосы 1…2 ГГц

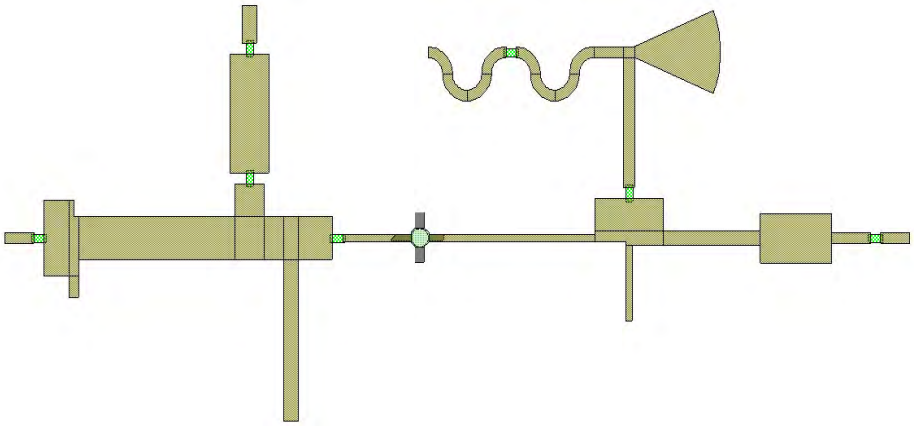


Рис. 3. Топология усилителя полосы 1…2 ГГц

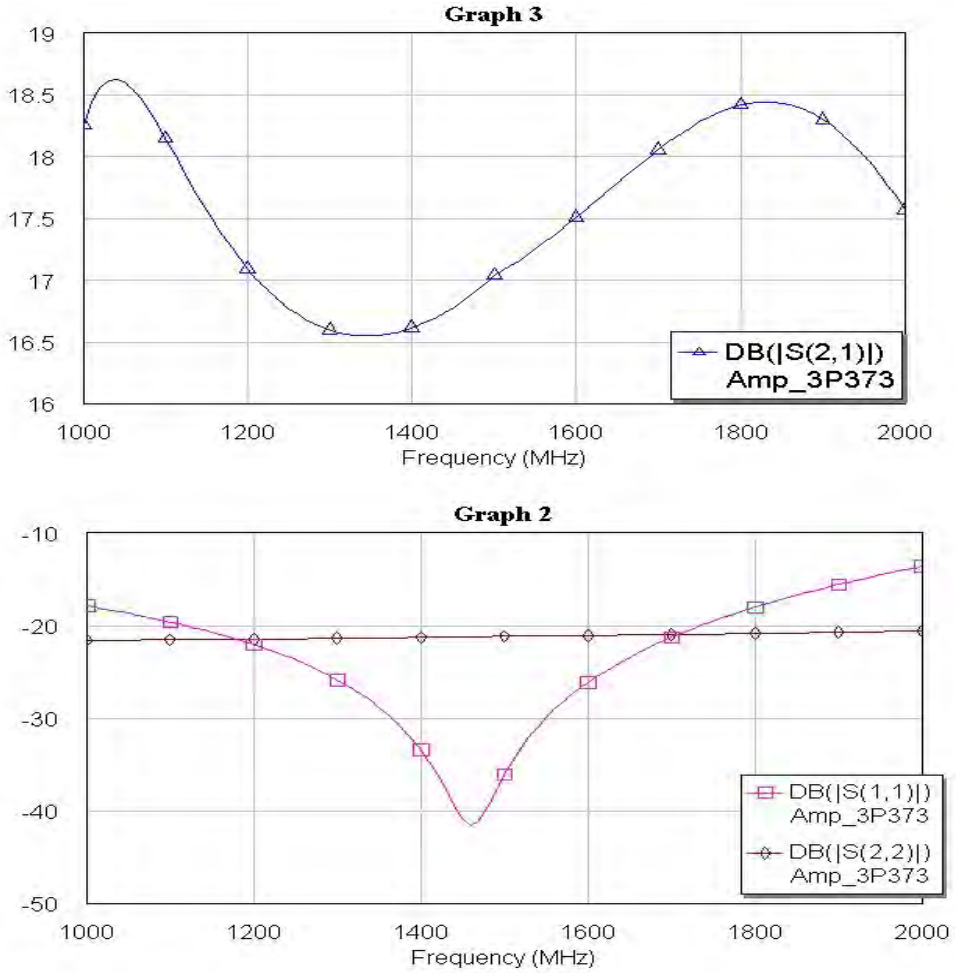


Рис. 4. Структура преселектора

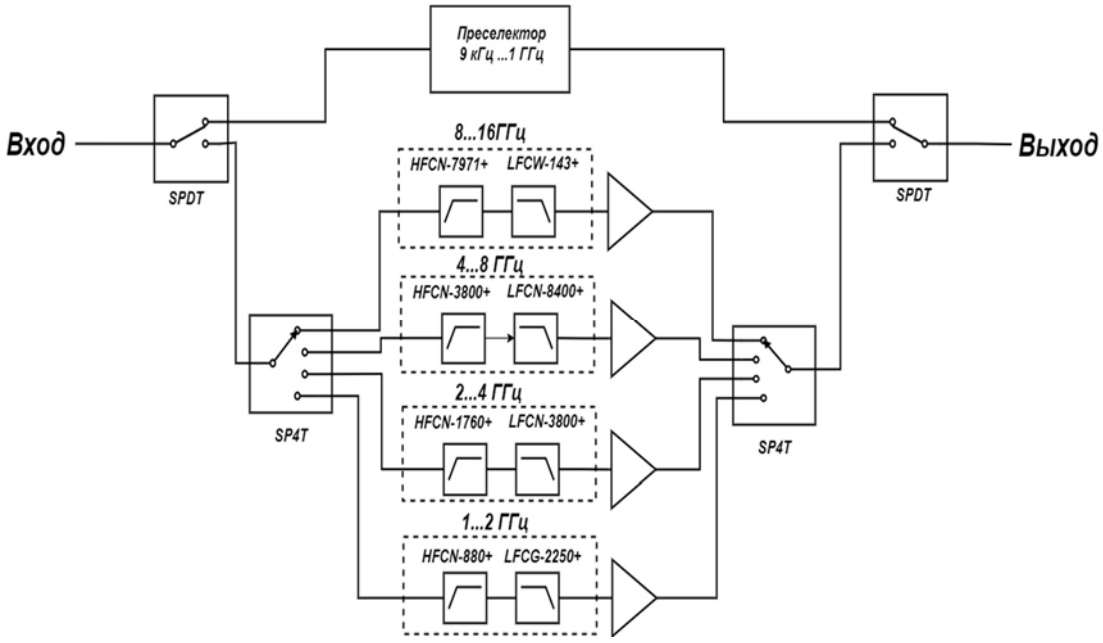


Рис. 5. Структура преселектора

Выводы

Предложена структура не дорогого и компактного преселектора, построенного с использованием усилителей, реализованных на отечественных СВЧ арсенид-галлиевых транзисторах. Коэффициент шума усилителей не превосходит 1 дБ. Коэффициенты усиления МШУ достаточны для компенсации потерь в последующих коммутаторах.

Список используемых источников

1. CISPR 16-1-1:2019 Specification for radio disturbance and immunity measuring apparatus and methods – Part 1–1: Radio disturbance and immunity measuring apparatus – Measuring apparatus. URL: https://docs.cntd.ru/document/1200142704

2. ГОСТ CISPR/TR 16-2-5-2019. Требования к аппаратуре для измерения радиопомех и помехоустойчивости. URL: https://docs.cntd.ru/document/1200142704

3. Schwarzbeck D. The EMI-Receiver according to CISPR 16-1-1 // Schwarzbeck Mess-Elektronik. URL: http://www.schwarzbeck.de/appnotes/EMIRcvrCISPR16.pdf

4. Рекомендация МСЭ-R M.1177-4 (04/2011) Методы измерения нежелательных излучений радиолокационных систем. Серия M Подвижная спутниковая служба, спутниковая служба радиоопределения, любительская спутниковая служба и относящиеся к ним спутниковые службы.

5. Раушер К., Йанссен Ф., Минихольд Р. Основы спектрального анализа. М. : Горячая линия-Телеком, 2006. 224 с.

6. Перестраиваемые полосно-пропускающие жиг фильтры ФФЛК2-17, ФКИН3-180-4.http://magneton.ru (скачивание 27.03.2021).

7. https://www.minicircuits.com/WebStore/RF-Filters.html (скачивание 27.03.2021).

8. https://www.analog.com/media/en/technical-documentation/data-sheets/hmc641lp4.pdf (дата обращения: 27.03.2021).

9. Mohamed Ribate, Jamal Zbitou, Rachid Mandy, Ahmed Erki. Broadband GaAs FET power amplifier for L and S bands applications // International Journal of Intelligent Engineering and Systems. October 2018.11(5):96-104.

10. BFR843EL3 Low noise broadband pre-matched RF bipolar transistor (дата обращения: 28.03.2021).

11. Полевые СВЧ транзисторы // Планета-Аргалл. URL: http://argall.ru/priemka_5.html (дата обращения 28.03.2021).

УДК 621.3, 681.5, 004.5, 608.4
ГРНТИ 59.14, 47.14, 20.53.23, 28.15.15,76.13.99

ОСНОВНЫЕ АСПЕКТЫ СОЗДАНИЯ УПРАВЛЯЕМОГО АНТРОПОМОРФНОГО ПРОТЕЗА С ПОМОЩЬЮ ОБРАБОТКИ И ПЕРЕДАЧИ ЭЛЕКТРИЧЕСКИХ СИГНАЛОВ ОТ МОЗГА

Г. С. Великоборец, В. А. Юрова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В медицинской технике особый интерес представляет разработка антропоморфных протезов конечностей для реабилитации пациентов. Для облегчения работы с протезом и управления им актуальным является проектирование интерфейса управления, основанного на передаче сигналов электромагнитным или электромеханическим путем. В работе рассмотрены основные направления в развитии таких интерфейсов, представлены результаты разработки интерфейса и технических средств управления роботизированной антропоморфной рукой, которая была разработана на предыдущем этапе работы и может быть использована в качестве медицинского протеза утраченной конечности или частью автоматизированной системы, имитирующей работу человеческой руки.

медицинская электроника, полупроводниковая электроника, антропоморфный протез, робототехника, роботизированные системы.

В профилактической и восстановительной медицине наблюдается переход на электромеханические протезы утраченных конечностей. С целью повышения точности воспроизводимых протезом действий возрастает сложность конструкции, современные технологии позволяют делать их более антропоморфными и легкими по весу, автономными в работе. Для облегчения работы с протезом ведутся наработки по созданию интерфейсов управления, которые различаются по типам используемых сигналов (речевой, электромагнитный и т. п.) и методов их обработки и передачи для воспроизведения действий протезом. Технология интерфейса мозг-компьютер (ИМК) была впервые разработана как инструмент, обеспечивающий базовое взаимодействие, такое как общение, без движения. Детально анализируя основные направления в разработках современных интерфейсов мозг-компьютер, их можно разделить на четыре основных группы:

1) Речевые интерфейсы мозг-компьютер;

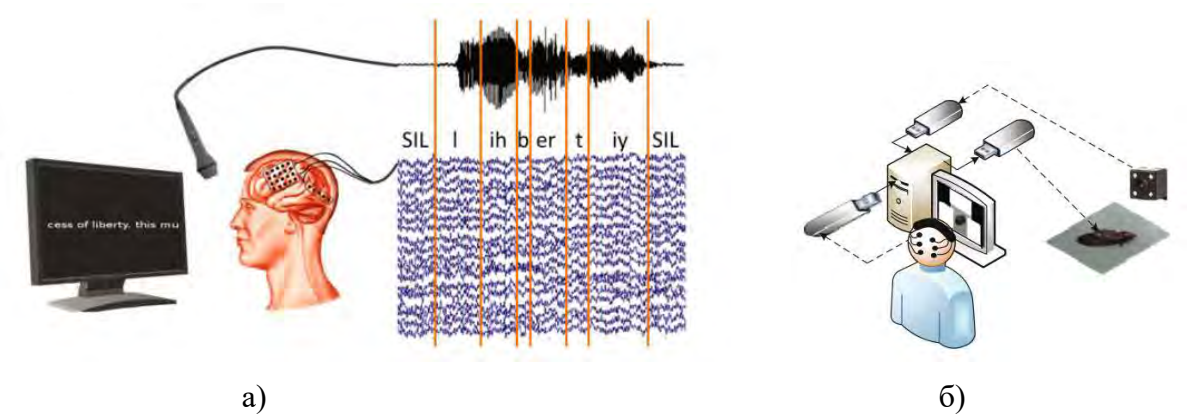
2) Моторные интерфейсы;

3) Интерфейсы для управления киборгами (чипирование живых организмов);

4) Интерфейсы для реабилитации.

Рассмотрим подробнее основные принципы работы этих интерфейсов для возможности управления спроектированной антропоморфной роботизированной рукой [1] с помощью обработки сигнала речи. Речевые интерфейсы мозг-компьютер (ИМК) основаны на распознавании непрерывной речи, которая преобразуется в электрические импульсы, подаваемые на управляемые устройства. Поскольку непрерывная речь обеспечивает очень естественный подход к общению, долгое время стоял вопрос, можно ли разработать ИМК, которые распознают речь по активности коры головного мозга. Такое решение обеспечивает возможность простой, быстрой и прямой передачи управляющего сигнала, например, на протезы конечностей или автоматизированные системы управления. Существуют экспериментальные подтверждения, что непрерывная речь может восприниматься мозгом как последовательность фонем (звуков). Эти фонемы могут быть декодированы из записей электрокортикографии (ЭКоГ) и позволяют составить произнесенные слова.

В эксперименте [2] авторы одновременно записывали ЭКоГ-активность и форму звуковой волны, в то время как участники читали вслух разные тексты. Авторы согласовали нейронные данные по времени с маркировкой фонем, полученных из звуковых данных, с помощью собственного инструментария распознавания речи BioKIT. Это позволило идентифицировать нейронную активность, соответствующую производству каждой фонемы (рис. 1, а). Затем авторы объединили фонемное (звуковое) представление корковой активности с языковой информацией из словаря, используя технологию автоматического распознавания речи, чтобы реконструировать слова в мысленно произнесенных фразах. Результаты этих исследований показывают, что с ограниченным набором слов в словаре интерфейс может восстанавливать полные предложения. Например, последовательность воображаемых фонем (звуков): *w/ih/aa/r/ /k/aa/m/ih/t/aa/t/ /t/aa/t/eh*/ интерфейс распознает и произнесёт как *We are commited today*. Здесь следует отметить, что для реализуемого проекта недостатком использования такого интерфейса в некоторых применениях может быть связано с дополнительными источниками звукового сигнала, например, других людей, общающихся рядом, что может привести к созданию неконтролируемых движений прототипа роботизированной руки, связанных с помехами от дополнительных источников.



а) б)

Рис. 1. Фонемное представление речи [2] (а) и интерфейс мозг-компьютер, управляющий киборгом [3] (б)

Также в работе была рассмотрена группа ИМК, представляющие собой моторные интерфейсы, одной из основных задач которых является разработка усовершенствованных нейронно-контролируемых протезов для восстановления или замены двигательной функции у пациентов с параличом верхней конечности. Чтобы создать высокоэффективный моторный ИМК, необходимо понимать, как сигналы, полученные от нервных имплантатов, кодируют грубые и тонкие движения верхних конечностей. Исследования показали [4], что сигналы ЭКоГ, записанные с сенсомоторной коры головного мозга человека, могут быть использованы для онлайн-контроля движений отдельных пальцев на подвижной протезной руке. Это открывает новые возможности нейронного контроля протезных конечностей для выполнения более тонких движений рук. Анализируя точность декодирования нейронных активаций, было обнаружено, что, вероятно, моторные ИМК могут обеспечить индивидуальный контроль пальцев даже при отсутствии сенсорной афферентной информации, например, в случае пациентов с травмами спинного мозга. Основным недостатком использования такой системы является необходимость вживления платы приема-обработки сигналов мозг-компьютер, что может вызывать сопутствующие осложнения у пациентов, связанные с качеством его установки, заживления ран после операции и дальнейшего приживания имплантата как инородного тела в организме.

Ещё одним типом, требующим вживления платы приема-обработки сигналов мозг-компьютер, являются интерфейсы для управления киборгами. Интерфейс мозг-компьютер, управляющий киборгом: представляет собой функциональный интерфейс мозг-мозг между человеком и, например, тараканом (см. рис. 1, б). В этом направлении разработок ИМК «киборг» был создан путем хирургического соединения портативного микростимулятора с нервами антенн живого таракана. Применяя специальную микростимуляцию, киборгом можно дистанционно управлять. Намерение движения может быть получено из человеческого мозга через ИМК. Электроэнцефа-

лография (ЭЭГ) на основе установившегося визуального вызванного потенциала в качестве надежного ИМК использовалась для передачи намерений человека изменять направление движения киборга.

Результаты экспериментов [3] показали, что средние показатели успешности работы ИМК по управлению киборгом путем считывания сигналов от человеческого мозга в одном решении превышали 85 %. Киборгом можно было успешно управлять через человеческий мозг, чтобы он мог пройти по заранее заданным дорожкам с 20 % успешностью.

Основной целью многих направлений ИМК является помощь в реабилитации. Например, большинство методов реабилитации после хирургического вмешательства основаны на периферической реорганизации моторного контроля, инициируемой периферической физиотерапией. В случае диагноза церебрального паралича (ЦП) имеет место поражения структуры мозга, когда периферическая нервная система и центральная нервная система должны быть интегрированы в физиотерапевтическую и когнитивную реабилитационную терапию. Именно такой подход предлагается в этом направлении создания ИМК. В [5] предложена система ИМК, состоящая из двух этапов: первая – как повторное обучение корковой активности, связанной с походкой, второй – активный контроль реабилитационной терапии на роботизированной платформе для пациентов с ЦП, перенесших многоуровневую ортопедическую хирургию. Таким образом, первый месяц после операции, когда пациент обездвижен, является наиболее подходящим периодом для подготовки мозга к новым образцам походки, которые позже будут развиваться в процессе физической реабилитации с помощью роботов. С таким подходом удаётся снизить период реабилитации до 2 месяцев. Экспериментальные исследования в этом направлении показали, что существуют способы реализации мысленного управления протезом посредством сигналов головного мозга, обрабатываемых ИМК.

Рассмотрев и проанализировав основные методы и их реализацию в создании интерфейсов мозг-машина. Для спроектированной роботизированной руки [1] в качестве интерфейса мозг-машина был разработан и собран двухэлектродный энцефалограф, на основе каскада из инструментальных усилителей AD620 (рис. 2).

В качестве электродов было решено использовать активные штырьковые электроды с буферным повторителем для согласования сопротивлений (рис. 2), так как большинство стандартных электродов должны плотно прилегать к поверхности головы и, следовательно, должны отсутствовать волосы.

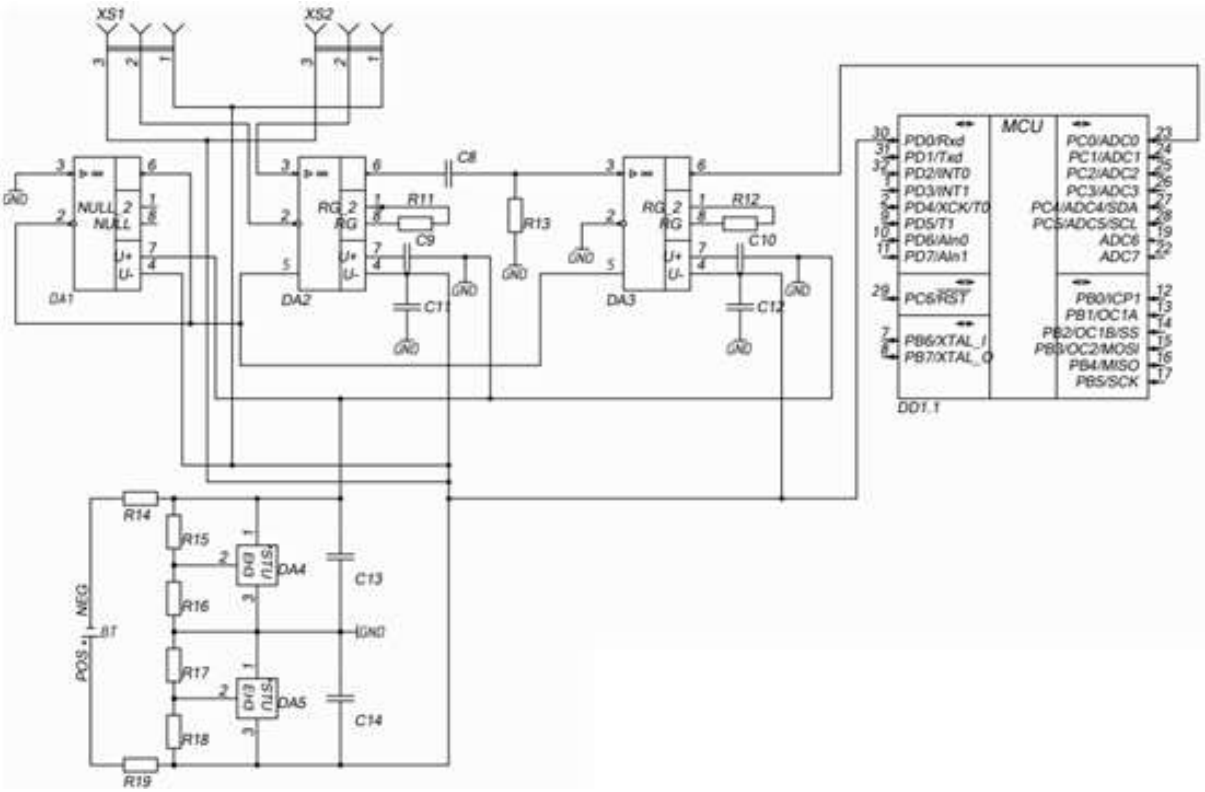
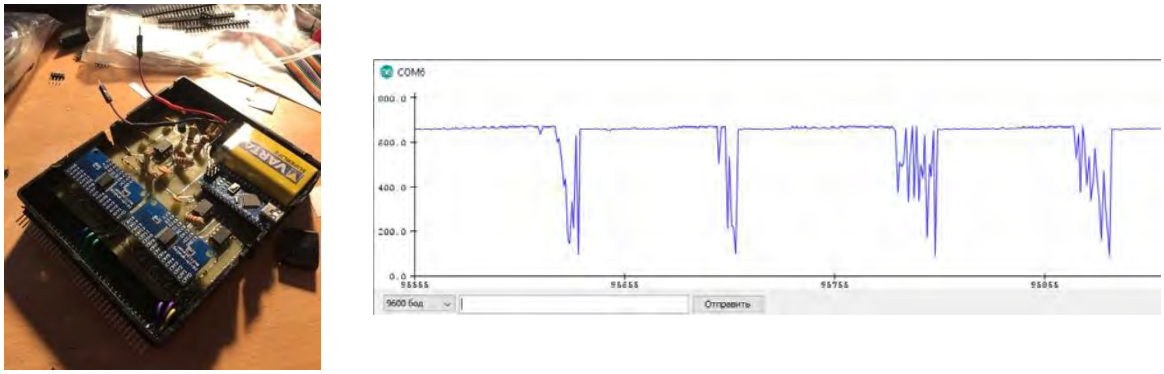


Рис. 2. Схема спроектированного двухэлектродного энцефалографа

На рис. 3, а представлен спроектированный и собранный энцефалограф. Результаты его тестирования показали, что возможно считывание сигналов мозговой активности с поверхности головы неинвазивным способом. Удалось добиться четкой реакции устройства на слабые моргания (рис. 3, б) [6]. В дальнейшем предполагается аппаратно-программная доработка соединения протеза и энцефалографа для полной реализации, управляемой антропоморфной роботизированной руки через интерфейс мозг-компьютер.



а) б)

Рис. 3. ЭЭГ (а), реакция ЭЭГ на моргание (б)

Список используемых источников

1. Великоборец Г. С., Юрова В. А. Создание системы управления антропоморфной роботизированной рукой // 74-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2020»: сб. науч. ст. Спец. вып. СПб. : СПбГУТ, 2020. С. 59–64.
2. Christian Herff, Adrianade Pesters, Dominic Heger, Peter Brunner, GerwinSchalk and Tanja Schultz. Towards Continuous Speech Recognition for BCI // Brain-Computer Interface Research, Springer Briefs in Electrical and Computer Engineering. doi 10.1007/978-3-319-57132-4_3.
3. Guangye Li, Dingguo Zhang. Brain-Computer Interface Controlling Cyborg: A Functional Brain-to-Brain Interface Between Human and Cockroach // Springer Briefs in Electrical and Computer Engineering. doi 10.1007/978-3-319-57132-4_6.
4. Tessy M. Lal, Guy Hotson, Matthew S. Fifer, David P. McMullen. Brain-Machine Interface Development for Finger Movement Control // Springer Briefs in Electrical and Computer Engineering, DOI 10.1007/978-3-319-57132-4_4.
5. J. Ignacio Serrano, M. D. del Castillo, C. Bayón, O. Ramírez, S. Lerma. BCI-Based Facilitation of Cortical Activity Associated to Gait Onset After Single Event Multi-level Surgery in Cerebral Palsy. Springer Briefs in Electrical and Computer Engineering. doi 10.1007/978-3-319-57132-4_8.
6. Великоборец Г. (2021) ЭЭГ, реакция на моргание [Любительское видео] // YouTube. 23 марта. URL: https://youtu.be/tK1Tmm5OrM8

УДК 621.372.8
ГРНТИ 47.45.31

ШИРОКОПОЛОСНОЕ ВОЗБУЖДЕНИЕ КРУГЛОГО ВОЛНОВОДА СПИРАЛЬНОЙ СТРУКТУРОЙ

Н. И. Глухов, К. А. Лепихин, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа посвящена теме широкополосного возбуждения круглого волновода. Главной задачей исследования является доказательство возможности возбуждения основных электродинамических мод круглого волновода в широком диапазоне частот. В качестве элементов питания волновода рассматриваются спиральные структуры, форма излучателей которых представлена в виде круговой, квадратной и треугольной индуктивностей. Приведены результаты электродинамического моделирования ряда моделей, а также результаты экспериментов.

широкополосное возбуждение круглого волновода, спиральные антенны, СВЧ.

В настоящее время волноводные тракты являются неотъемлемой частью таких сложных систем как радиолокационные, спутниковые и радиорелейные. Поэтому переходы от длинных линий к волноводам являются основным, составным элементом, который определяет качество системы в целом.

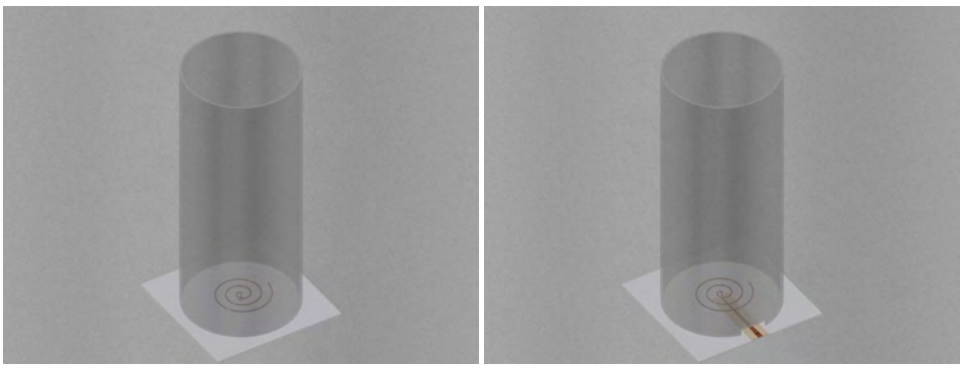
В литературе по электродинамике много материала о возбуждении волноводов в узкой полосе частот. Исторически, в качестве первого питающего элемента волноводов использовался штырь. Потом была предложена возможность возбуждения электродинамических мод в волноводе посредством рамки. Одним из недостатков волноводных систем при использовании данных питающих элементов является малый рабочий частотный диапазон, определяющийся в первую очередь геометрией самих излучателей, возбуждающих волновод.

Расширение рабочего диапазона, в том числе и волноводных систем, является актуальной задачей. Данную задачу предлагается решить с помощью использования спиральных излучателей, помещенных в волновод, одной из главных характеристик которых является широкополосность [1, 2, 3].

В материале [4, 5] приводится математическое описание волнового сопротивления круглой рамки, возбуждающей моды (TE01, TE11, TM11 и др.) в круглом волноводе. Исходя из расчетов [4, 5], при определенных пространственных условиях волновое сопротивление круглой рамки становится равным порядка 180 Ом, что коррелирует с теорией спиральных структур. Тем самым можно предположить, что использование спиралей в качестве элементов питания круглого волновода в широком диапазоне частот целесообразно.

Объектами исследования в данной работе были несколько моделей круглых волноводов с длинной металлических стенок порядка 500 мм и с диаметрами основания 150, 125, 100 мм соответственно, каждая модель была изготовлена и исследована. В качестве питающих узлов выступают планарные спиральные структуры, изложенные в материале [6], форма излучателей которых представлена в виде круговой, квадратной и треугольной индуктивностей [7], заключенных внутри окружности одного и того же радиуса. Диапазоны частот, в которых проводится анализ волноводных систем составляет 2–4 и 1–6 ГГц.

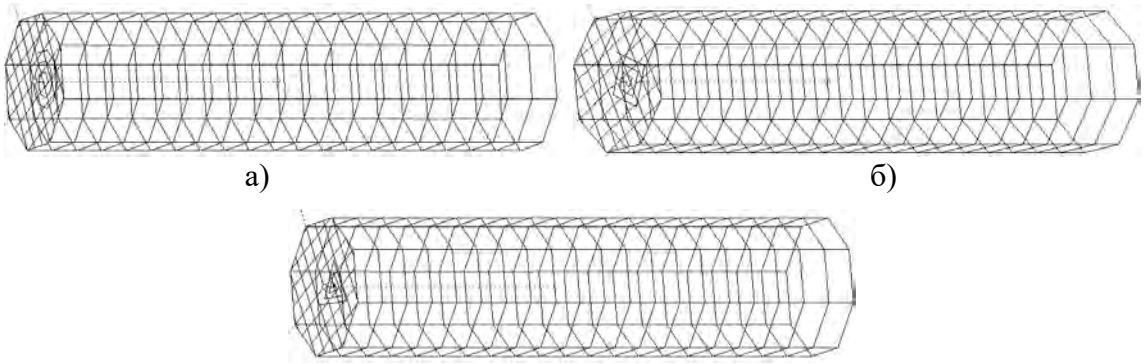
В ходе исследования рассматривались два способа питания спиральных излучателей, помещаемых в волновод (рис. 1 а, б).



а) б)

Рис. 1. Эскизы рассматриваемых способов питания круглого волновода спиральными структурами: а) коаксиальное, б) с помощью микрополосковой линии

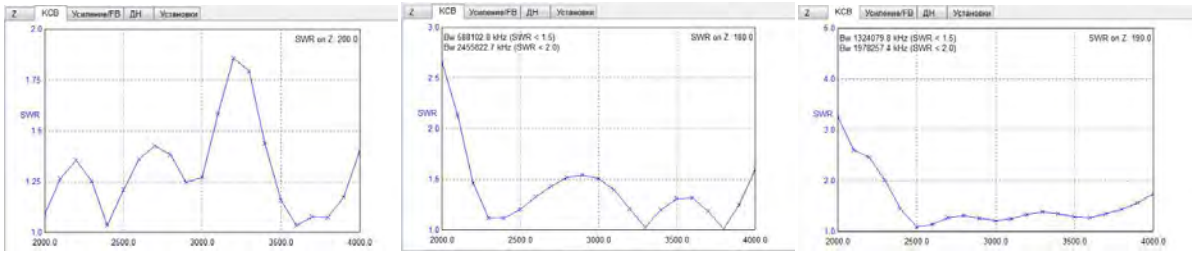
Электродинамическое моделирование, выполненное в программе MMANA-GAL, представлено для ряда моделей с диаметром волноводов 125 мм и длиной металлических стенок 500 мм в диапазоне частот 2–4 ГГц (рис. 2).



а) б)

в)

Рис. 2. Электродинамические модели ряда волноводных структур



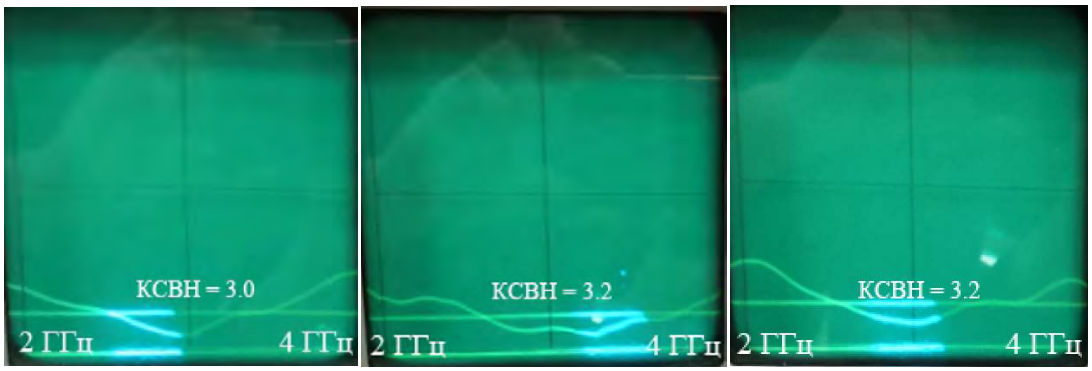
а) б) в)

Рис. 3. Результаты электродинамического моделирования моделей (рис. 2 а, б, в, соответственно)

Из оценки результатов электродинамического моделирования (рис. 3 а, б, в) можно предположить, что широкополосное возбуждение круглого волновода спиральными структурами возможно.

Результаты ряда экспериментов при коаксиальном питании волноводных структур (рис. 1 а) для диаметра волновода 125 мм с длиной металлических стенок порядка 500мм в диапазоне 2–4 ГГц, проводимых на базе СВЧ лаборатории СПбГУТ, представлены ниже.

Рис. 4. 3D модель сборочного комплекса макетов с диаметром волновода 125 мм



а) б) в)

Рис. 5. ЧХ КСВН макетов (рис. 4) с различными питающими элементами волновода: а) круговая СА, б) квадратная СА, в) треугольная СА

В ходе экспериментов установлено, что все волноводные структуры работоспособны (рис. 4), волна на открытом конце волноводов излучается в пространство. Как видно из графиков на рис. 5 а, б, в ЧХ КСВН всех волноводных структур практически равномерное во всем исследуемом диапазоне частот 2–4 ГГц, что говорит о их широкополосном возбуждении. Стоит также отметить, что согласование питающей коаксиальной линии со спиральной антенной отсутствовало, выходное волновое сопротивление фидера равно 50 Ом.

Результаты ряда экспериментов при питании волноводных структур с помощью микрополосковой линии (рис. 1б) для диаметров волноводов 150, 125, 100 мм соответственно, с длинами металлических стенок порядка

500 мм в диапазоне 1–6 ГГц, проводимых с использованием векторного анализатора ARINST VNA-PR1, представлены ниже.

В ходе экспериментов установлено, что все волноводные структуры рабочие (рис. 6), волна на открытом конце волноводов в исследуемом диапазоне 1–6 ГГц излучается в пространство при различных диаметрах макетов волноводов с различными питающими узлами.

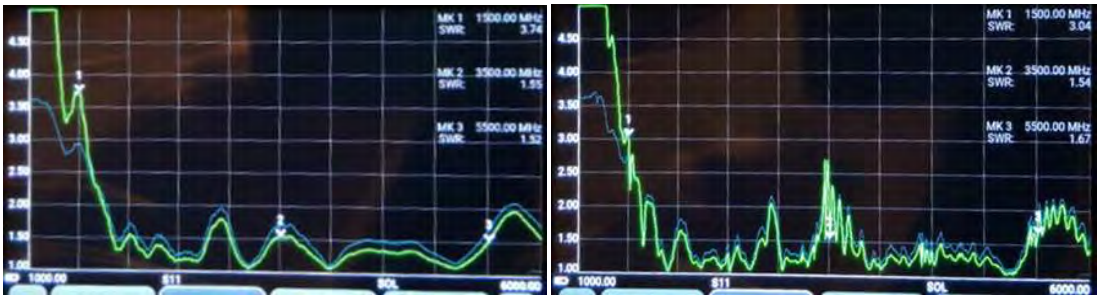
Рис. 6. 3D модель сборочного комплекса макетов
с различными диаметрами волноводов 150, 125, 100 мм

Из графиков ЧХ КСВН (рис. 7 б, в, г; рис. 8 б, в, г; рис. 9 б, в, г) видно, что средний уровень КСВН в рабочей полосе частот находится в приемлемом диапазоне, что доказывает возможность широкополосного возбуждения волноводов спиральными структурами.

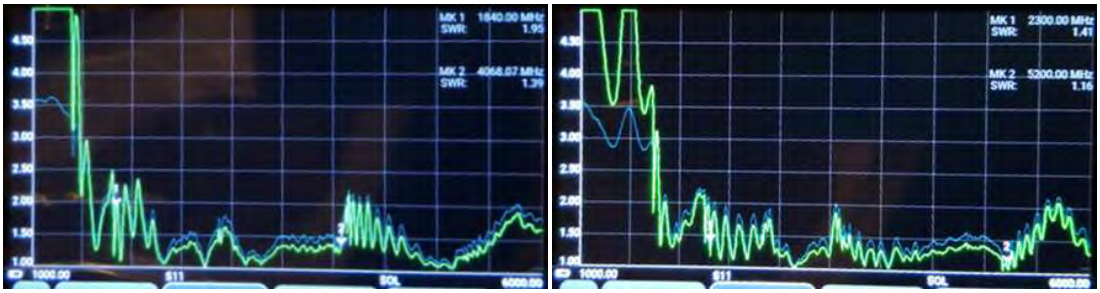
Участки, на которых ярко выражена нестабильность волноводных структур (рис. 7 б, в, г; рис. 8 б, в, г; рис. 9 б, в, г), проявляющаяся в виде частых синусоидальных всплесков КСВН, с теоретической точки зрения возникают на частотах, соответствующих критическим длинам волн мод. Маркерами МК 1, МК 2, МК 3 на графиках (рис. 7 б, в, г; рис. 8 б, в, г; рис. 9 б, в, г) обозначены места критических частот для мод E01, E02, E03, соответственно.

Также предполагается, что поляризация бегущей электромагнитной волны внутри волновода такая же, как и у спиральной антенны, т. е. эллиптическая [6].

Таким образом, результатом данной работы является доказательство возможности возбуждения различных электродинамических мод в круглом волноводе в широком диапазоне частот питающим элементом в виде спирали.

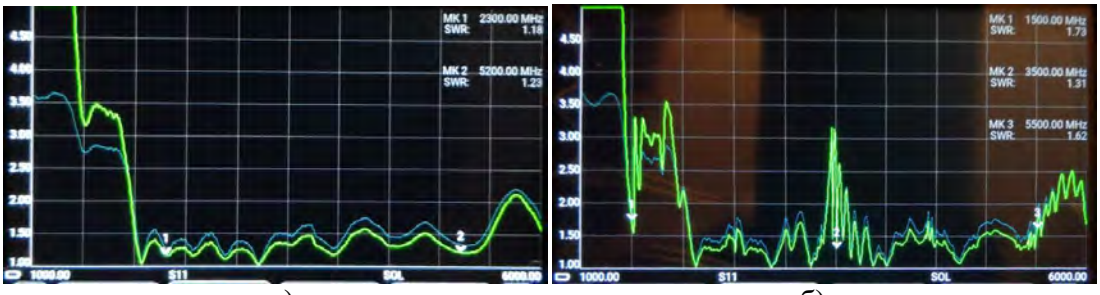


а) б)

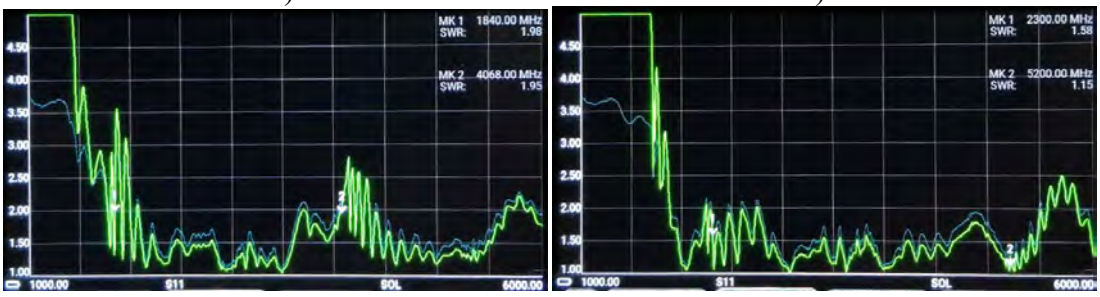


в) г)

Рис. 7. ЧХ КСВН волноводных структур, питающим узлом является круговая СА: а) СА над открытой проводящей поверхностью; б), в), г) СА помещена в волноводы диаметрами 150, 125, 100 мм соответственно

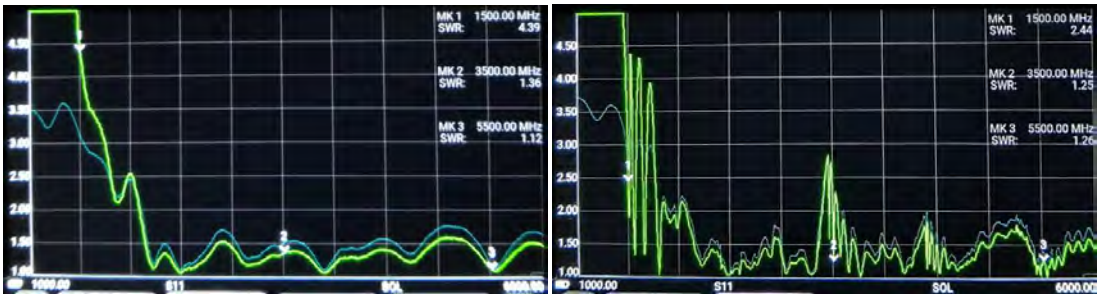


а) б)

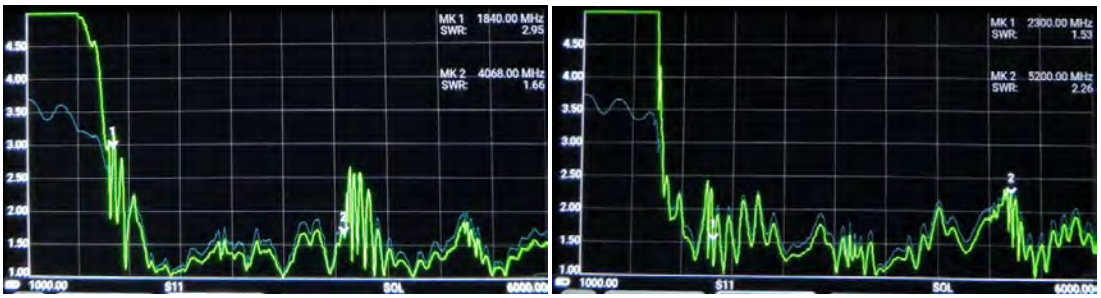


в) г)

Рис. 8. ЧХ КСВН волноводных структур, питающим узлом является квадратная СА: а) СА над открытой проводящей поверхностью; б), в), г) СА помещена в волноводы диаметрами 150, 125, 100 мм соответственно



а) б)



в) г)

Рис. 9. ЧХ КСВН волноводных структур, питающим узлом является треугольная СА: а) СА над открытой проводящей поверхностью; б), в), г) СА помещена в волноводы диаметрами 150, 125, 100 мм соответственно

Список используемых источников

1. Юрцев О. А., Рунов А. В., Казарин А. Н. Спиральные антенны. М.: Советское радио, 1974. 224 с.

2. Сазонов Д. М. Антенны и устройства СВЧ. Учебник для радиотехнических специальностей вузов. М.: Высшая школа, 1988. 432 с.

3. Рамзай В. Частотно-независимые антенны. М.: МИР, 1968. 172 с

4. Seshadri, S. R. Resistance of a circular loop with dipolar current distribution in a cylindrical waveguide // Proceedings of the IEEE. 1980. Vol. 68. Pp. 1012–1014.

5. Seshadri, S. R. Resistance of a circular current loop in a cylindrical waveguide // Proceedings of the IEEE. 1980. Vol. 68. Pp. 1014–1015.

6. Бочаров Е. И., Лепихин К. А., Седышев Э. Ю. Исследование спиральных структур с экраном // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. Санкт-Петербург, 2020. С. 404–407.

7. Вяльшин Э. С., Криворука О. О., Лепихин К. А., Седышев Э. Ю. Спиральные антенны СВЧ диапазона // Проектирование и технология электронных средств. 2020. № 3. С. 18–26.

УДК 621.317.7.023
ГРНТИ 45.03.07

АНАЛИЗ РАБОТЫ АНАЛОГО-ЦИФРОВОГО ПРЕОБРАЗОВАТЕЛЯ ПАРАЛЛЕЛЬНОГО ТИПА ДЛЯ ОПРЕДЕЛЕНИЯ ДЕЙСТВУЮЩЕГО ЗНАЧЕНИЯ НАПРЯЖЕНИЯ ПРИ НАЛИЧИИ ВО ВХОДНОМ СИГНАЛЕ ВЫСШИХ ГАРМОНИК

Е. В. Казакевич, К. А. Однокурцев, П. В. Трепалин

Военная академия связи

Аналого-цифровые преобразователи широко используются для преобразования напряжения в цифровой код в различных электронных системах. Параллельные АЦП отличаются своим быстродействием, так как параллельная схема позволяет всем компараторам проводить измерения одновременно. Если входной сигнал содержит высшие гармоники, то его форма искажается относительно идеальной синусоидально формы и для корректного расчета напряжения нужно учитывать разрядность АЦП и его опорное напряжение.

высшие гармоники, действующее значение напряжения, аналого-цифровой преобразователь.

В качестве примера в статье рассмотрена модель 3-х разрядного АЦП в связи с более наглядной и простой в управлении схемой. На рис. 1 изображена принципиальная схема моделируемого АЦП. АЦП этого типа осуществляет квантование сигнала одновременно с помощью набора компараторов (*f*), включенных параллельно источнику входного сигнала. Каждый компаратор сравнивает входной сигнал со своим опорным напряжением (U_{REF}), получаемый с помощью делителя напряжения [1, 2].

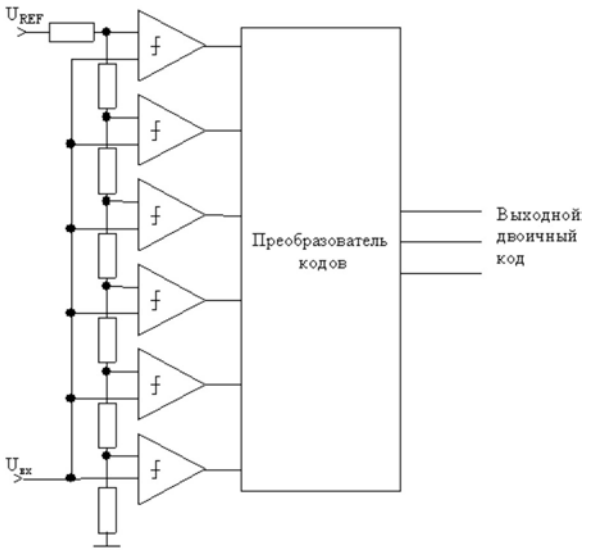


Рис. 1. Схема 3-х разрядного параллельного АЦП

Если U_{REF}<U_{vh}, то на выходе компаратора получается логическая единица, записывающаяся в старший бит. На вход преобразователя кодов поступает группа логических нулей и

единиц, которые обрабатываются в трехзначный двоичный код. С помощью трех двоичных разрядов можно представить восемь различных чисел.

Сигнал на входе обрабатывается с определенной частотой дискретизации (шагом). После чего двоичные коды, полученные на выходе, преобразуются в дискретный сигнал и по полученным точкам считается среднее квадратичное значение напряжения.

Моделирование параллельного АЦП представлено на рис. 2.

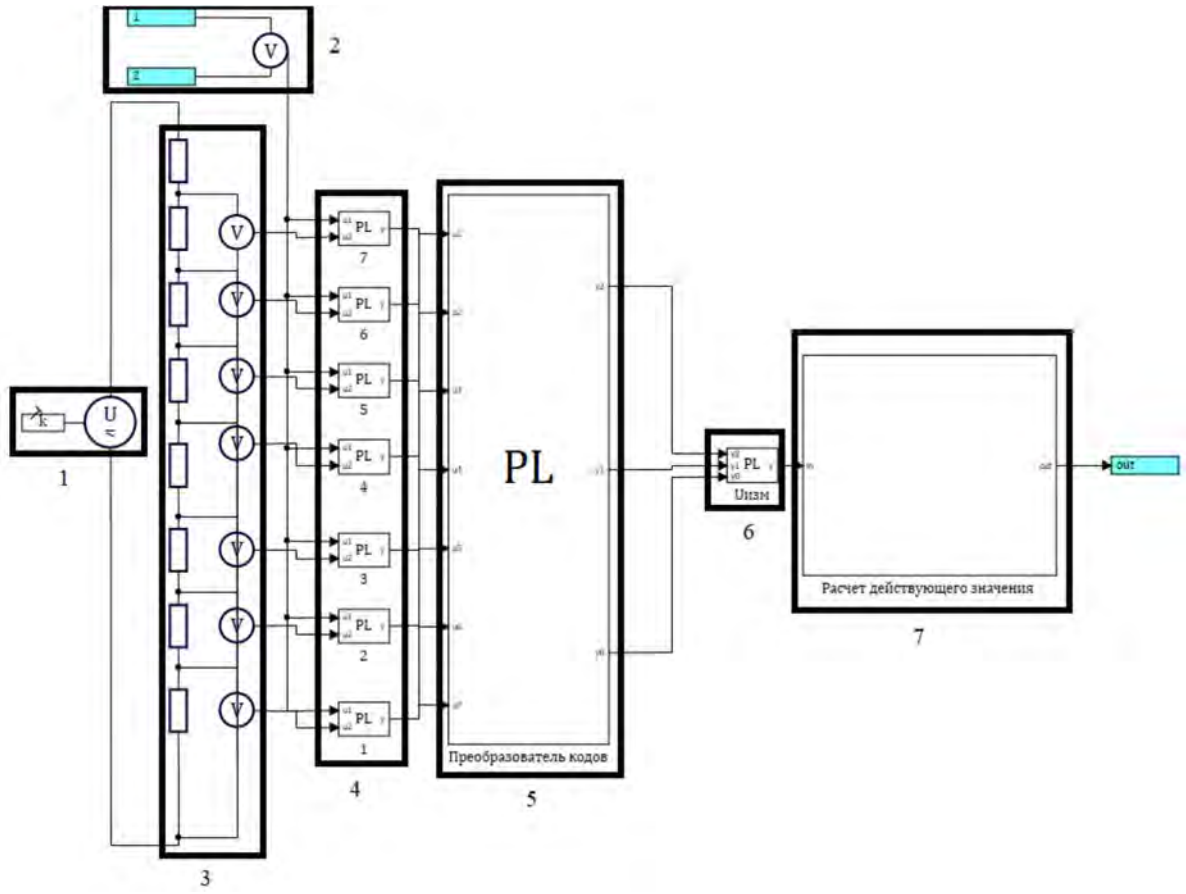


Рис. 2. Модель АЦП
1 – блок формирующий опорное напряжение, 2 – входной сигнал,
3 – делитель напряжения, 4 – массив компараторов, 5 – дешифратор,
6 – блок преобразования двоичного кода, 7 – блок расчета действующего значения

Опорное напряжение определяется производителем контроллеров, в данной схеме опорное напряжение моделируется источником постоянного напряжения (1), значение которого можно подстраивать. Входной выпрямленный сигнал (2) через делители напряжения – резисторы (3) подается на компараторы (4), которые моделируются программным блоком. После группа чисел подается на дешифратор (5). Полученный двоичный код подается на блок 6, который преобразует код в дискретное значение напряжения, которое записывается в блок 7, который по истечению заданного времени по полученным точкам считает действующее значение напряжения [3, 4].

Для расчета действующего значения напряжения используется метод Симпсона:

$$\int_a^b f(x)dx \approx \frac{h}{3}\left[f_0 + f_{2N} + 2\sum_{j=2,2}^{2N-2} f_j + 4\sum_{j=1,2}^{2N-1} f_j\right].$$

Данный АЦП проводит 40 измерений за один период основной синусоиды с шагом дискретизации h = 0,005. Опорное напряжение U_{REF} = 371 В.

Для анализа работы АЦП приведено 2 сигнала различного гармонического состава (рис. 3). В случае сигнала, а) 5-я и 7-я гармоники примерно равны и в сумме с 11-ой дают значительное искажение сигнала, который при недостаточной разрядности АЦП может быть некорректно обработан. А в случае сигнала б) 5-я гармоника дает пик, который превышает опорное напряжение АЦП. Из графиков видно, что наибольшее искажение вносят 5-я, 7-я, 11-я и 13-я гармоники.

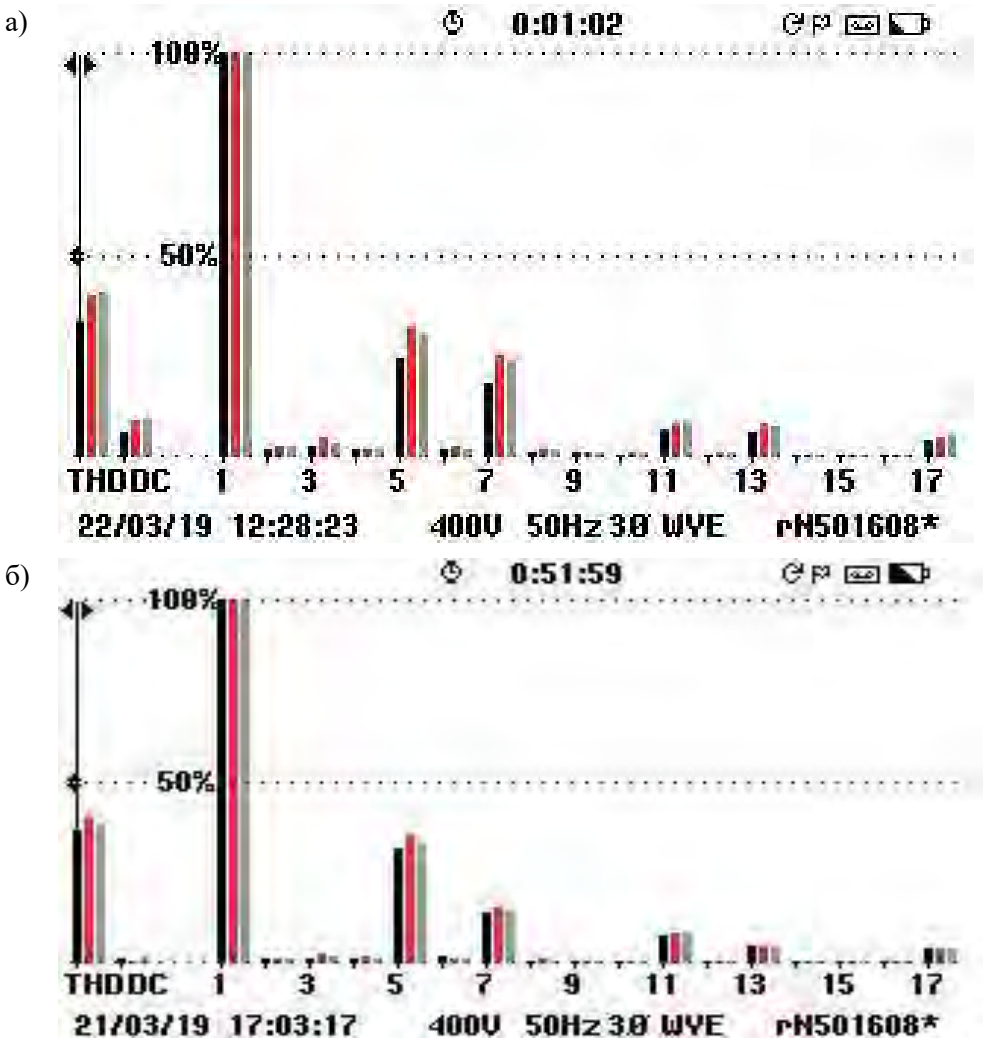


Рис. 3. Значение THD в сигнале

Результаты обработки входного сигнала АЦП представлен на рис. 4.

а)

б)

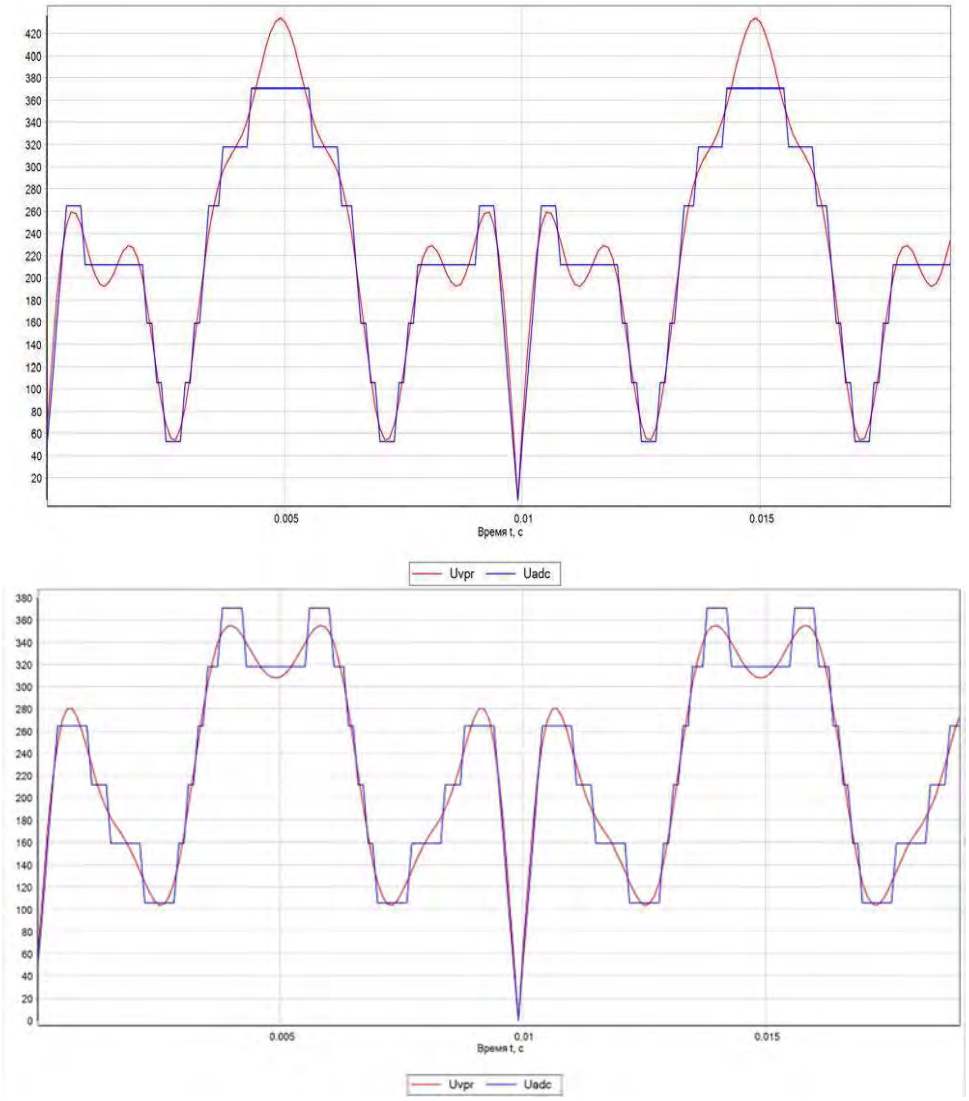


Рис. 4. Выпрямленное напряжение и значения сигнала АЦП

В обоих случаях сигнал на выходе АЦП будет некорректным, т. к. в случае сигнала а) АЦП завысит действующее значение сигнала из-за недостатка разрядности, а при сигнале б) из-за превышения опорного значения рассчитанное напряжение АЦП будет меньше реального.

В таблице (см. ниже) сведены результаты расчета действующего значения напряжения входного сигнала АЦП.

Полученные результаты моделирования показывают, что корректная работа АЦП зависит от составляющих входного сигнала. Реальное действующее входное напряжение в обоих случаях отличается от значения, рассчитанным АЦП.

Проблема недостаточной точности решается путем применения АЦП большей разрядности. Параллельные АЦП выпускаются в основном 8-ми разрядные. Существуют так же и 16-ти и 24-х разрядные АЦП.

ТАБЛИЦА. Полученные значения напряжения

Опыт при недостаточной разрядности АЦП		Опыт при недостаточном значении опорного напряжения	
$U_{rms\,real}$, В	239	$U_{rms\,real}$, В	242
$U_{rms\,adc}$, В	249	$U_{rms\,adc}$, В	231

где $U_{rms\,real}$ – реальное действующее значение напряжение,

$U_{rms\,adc}$ – действующее значение напряжение, рассчитанное АЦП.

Проблема, превышения опорного напряжения зависит, во-первых, от производителя контроллера, так как существует ряд стандартных значений. А во-вторых, применением делителя напряжения, причем при выборе делителя необходимо анализировать гармонический состав входного сигнала.

Список используемых источников

1. Горюнов А. Г., Ливенцов С. Н. Учебное пособие к выполнению лабораторной работы по дисциплине «Микропроцессорная техника» и курсового проекта по дисциплине «Электроника и микроэлектроника» для студентов ФТФ. Томск, 2004.

2. Хоровиц П., Хилл У. Искусство схемотехники: пер. Бронин Б. Н., Коротов А. И., Микшис М. Н., Поспелов Л. В., Соболева О. А., Чечеткин Ю. В. М.: Бином, 2020. 704 с. ISBN 978-5-9518-0351-1.

3. Behzad Razavi, Principles of Data Conversion System Design. Wiley, 1994.

4. Китаев В. В, Бокуняев А. А., Колканов М. Ф. Электропитание устройств связи. М.: Связь, 1975. 328 с.

УДК 621.373.52
ГРНТИ 47.45.99

МИКРОВОЛНОВЫЙ ГЕНЕРАТОР НА КОЛЬЦЕВОМ ЭЛЛИПТИЧЕСКОМ РЕЗОНАТОРЕ В СИММЕТРИЧНОМ ПОЛОСКОВОМ ИСПОЛНЕНИИ

Т. О. Каткова, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе предлагается конструкция СВЧ генератора на кольцевом эллиптическом резонаторе. Произведено компьютерное моделирование устройства в программе RFSimm99. Рассчитаны геометрические размеры устройства. Создан макет генератора на полосковой линии. Экспериментальные исследования показали полную работоспособность предлагаемой конструкции.

СВЧ генератор, активный двухполюсник, резонатор, спектрограмма.

Генераторы являются основой многих микроволновых устройств. Они могут быть разными по схемам, конфигурации и в разном конструктивном исполнении. Сегодня активно исследуются генераторы на резонаторах бегущей волны, предложенные в нашем Университете. В этих генераторах используются кольцевые эллиптические резонаторы, использующие различные активные элементы (транзисторы, туннельные диоды, диоды Ганна, лавинно-пролётные диоды и др.) [1, 2]. На рис. 1 представлена 3D-модель кольцевого эллиптического резонатора.

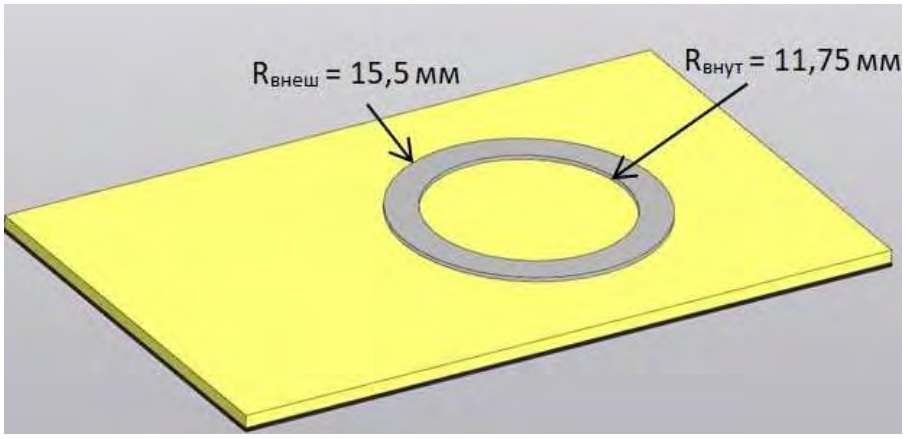


Рис. 1. Макет кольцевого резонатора

Для того чтобы исследовать предлагаемый генератор, 3D модель которого была построена в учебной версии Компас 3D и представлена на рис. 2,

проследим зависимость его выходных характеристик от параметров конструкции. Задающее кольцо возьмем из работы [1], изменив выходную линию и точку ее включения в кольцо.

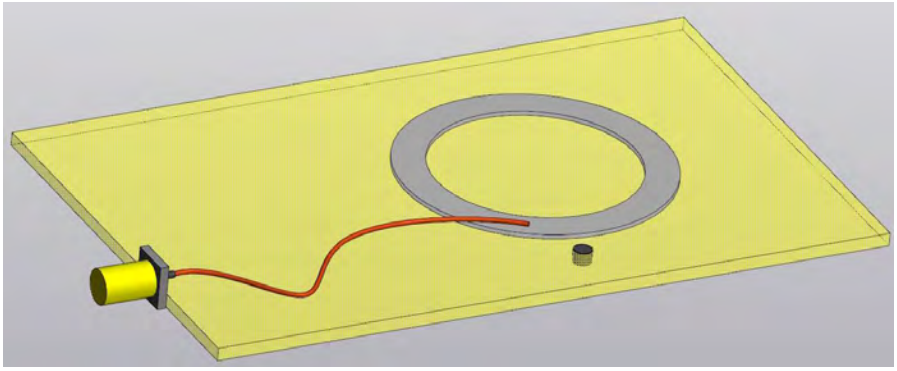


Рис. 2. 3D-модель СВЧ генератора

Первым этапом рассчитаем резонансные частоты выбранного кольца (рис. 1, 2). Расчет проведем по формулам (1)–(5), которые учитывают погонные параметры устройства, а также по формулам, которые учитывают кратность длины кольцевого резонатора длине волны в нем (учитывающие резонансную частоту с точки зрения геометрической оптики) [1]. Для начала рассчитаем ёмкость и индуктивность резонатора по формулам (1), (2):

$$C = \frac{\varepsilon_0 \cdot \varepsilon_{эфо} \cdot \pi \cdot (R_{внеш} - R_{внут})^2}{h} = 1{,}09 \text{ пФ}, \quad (1)$$

где $R_{внеш}$ – внешний радиус,

$R_{внут}$ – внутренний радиус,

h – толщина подложки.

$$L = \frac{\mu \cdot \mu_0 \cdot N^2 \cdot (R_{внеш} - R_{внут})}{2} = 2{,}355 \text{ нГн}, \quad (2)$$

где N – количество витков.

Отсюда найдём резонансную частоту с учётом погонных параметров:

$$f_{рез1} = \frac{1}{2 \cdot \pi \cdot \sqrt{L \cdot C}} = 3{,}14 \text{ГГц}, \quad (3)$$

Для расчёта частоты резонанса с точки зрения геометрической оптики необходимо найти длину волны по формуле:

$$\lambda = \frac{l_{\text{ср}}}{n} = 0{,}0855 \text{ м}, \quad (4)$$

где $l_{\text{ср}}$ – длина резонансного кольца,

n – количество бегущих волн, укладывающихся в данном кольце.

Тогда частота резонанса находится по формуле:

$$f_{\text{рез}} = \frac{c}{\lambda \cdot \sqrt{\varepsilon}} = 2{,}588\text{ГГц}, \quad (5)$$

Сравнивая результаты, полученные по двум формулам (3) и (5), имеем разницу почти в 1,2 раза, что обусловлено разным подходом к нахождению резонансной частоты.

Изготовив макет, представленный на рис. 3 (см. ниже), были проведены серии экспериментов, в итоге получена спектрограмма, представленная на рис. 4 (см. ниже). На ней видны три основных частоты генерации:

$$F_1 \approx 1{,}500 \text{ Гц}, F_2 \approx 3{,}100 \text{ Гц}, F_3 \approx 4{,}600 \text{ Гц}.$$

Частота резонанса, рассчитанная по формуле (1), учитывающей эквивалентные параметры кольца, совпадает с самой большой (–22 дБм) частотой генерации нашего макета.

Рис. 3. Макет СВЧ генератора

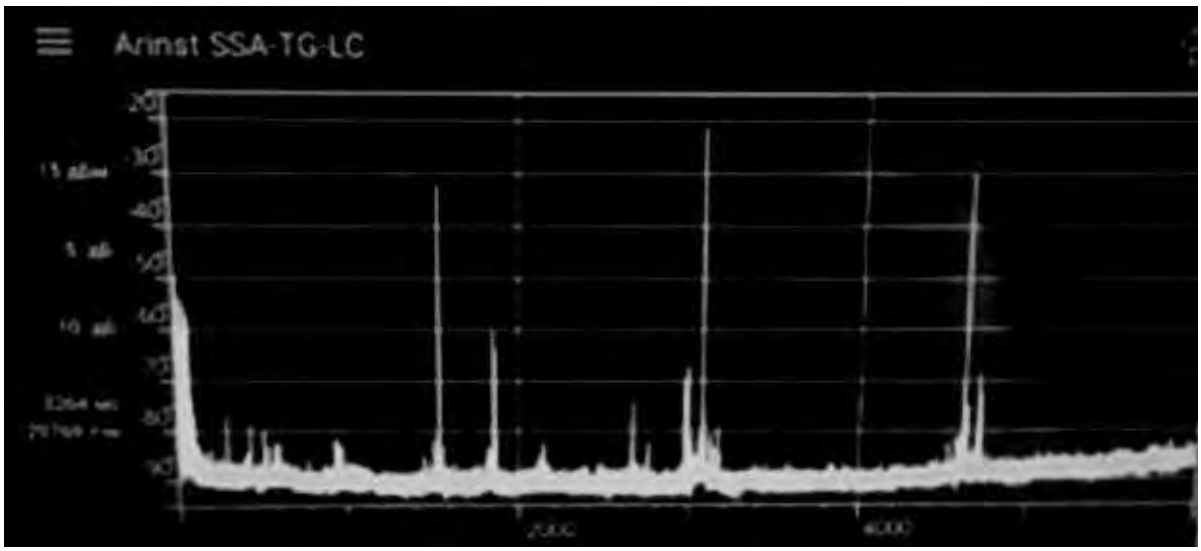


Рис. 4. Спектрограмма СВЧ генератора на кольцевом эллиптическом резонаторе

Макет генератора включает в себя активный двухполюсник (туннельный диод), отрицательное дифференциальное сопротивление которого компенсирует потери в кольце и собственно обеспечивает генерацию [3]. Особый интерес представляет построение эквивалентной схемы устройства. Предлагаемая схема показана на рис. 5. Сумма длин линий равна длине кольца из формулы (4). При моделировании в программе RFSimm99 диод заменяется резистором с отрицательным сопротивлением.

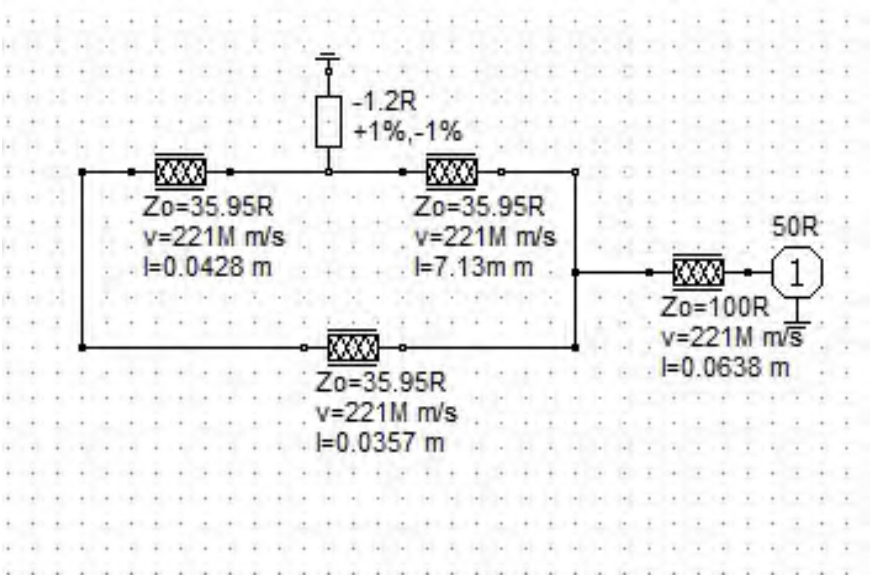


Рис. 5. Эквивалентная схема СВЧ генератора в САПР RFSimm99

Снять ВАХ СВЧ диода очень сложная задача, поэтому номинал резистора подбирался с учётом потерь в кольце, которые не столь велики. Были рассмотрены номиналы от –0,1 до –5 Ом. При значении номинала диода –1,2 Ом достигается наиболее правдоподобная характеристика исходного

макета. На рис. 6 представлена амплитудно-частотная характеристика в диапазоне (1–8) ГГц. Из АЧХ видно, что генерация происходит на частотах $F_1 \approx 1{,}273$ Гц, $F_2 \approx 3{,}907$ Гц, $F_3 \approx 6{,}388$ Гц.

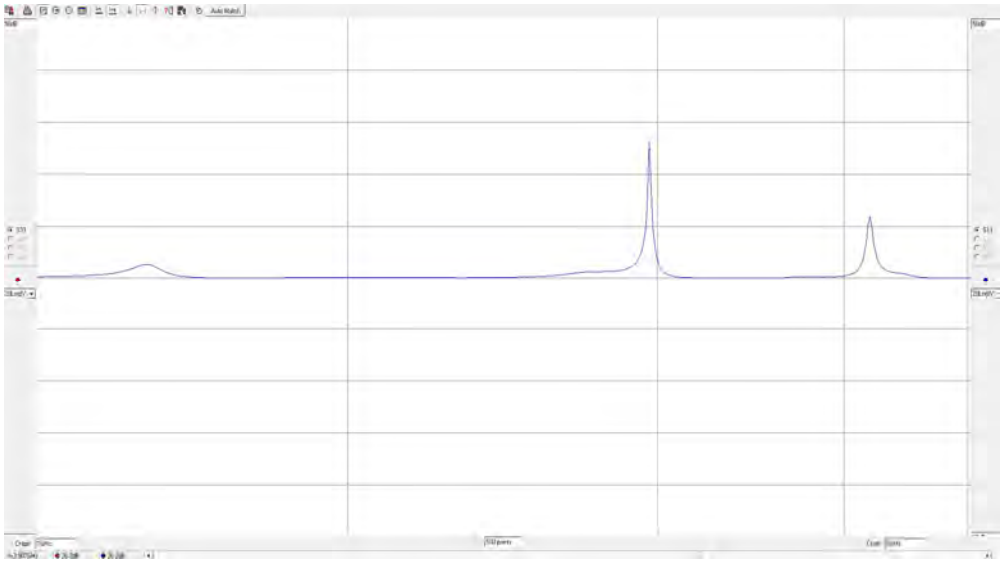


Рис. 6. S11 генератора с одним диодом

Результат эксперимента нельзя назвать однозначным. Макет генерирует три частоты, которые не удалось рассчитать точно, однако эквивалентная схема дает представление о характере генерации.

Итогом работы можно считать действующий макет генератора с «чистым» рабочим спектром и высоким уровнем выходной мощности основного колебания. Важно отметить, что уровень генерации по сравнению с устройством из работы [1] для данной конструкции во много больше.

Список используемых источников

1. Сазоненко Н. Ю., Седышев Э. Ю. Генератор на кольцевом резонаторе в микрополосковом исполнении // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. С. 509–513.

2. Янчук Е. В. Туннельные диоды в приемно-усилительных устройствах. М. : Энергия, 1967. 56 с.

3. Седышев Э. Ю., Шомин А. Ю. Исследование возможности одновременного использования нескольких активных двухполюсников при создании СВЧ генераторов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. С. 514–519.

УДК 621.373.52
ГРНТИ 47.45.33

СВЧ ГЕНЕРАТОР НА АКТИВНОМ ДВУХПОЛЮСНИКЕ В ЦИЛИНДРИЧЕСКОМ РЕЗОНАТОРЕ

Е. А. Коновалова, В. И. Мотренко, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Создание высокостабильных генераторов является актуальной задачей в области сверхвысоких частот. Предметом исследования является генератор на активном двухполюснике в цилиндрическом резонаторе. В работе произведён расчёт резонансных частот для трёх типов электромагнитных колебаний цилиндрического резонатора в зависимости от его геометрических размеров и заполнения. Создан экспериментальный стенд генератора, с помощью которого было проверено наличие генерации на рассчитанных частотах, приведены результаты, полученные в ходе эксперимента, и сделано сравнение результатов с расчётами.

СВЧ, генератор, цилиндрический резонатор.

Активное развитие микроволновой техники в последние годы обращает внимание разработчиков к объёмным цилиндрическим резонаторам [1, 2]. Данный тип резонаторов обладает меньшей добротностью, чем сферические [3], но выигрывает за счёт более простого и дешёвого процесса производства. Одним из достоинств цилиндра является возможность использования в качестве резонатора его сегментов.

Целью работы является создание высокостабильного генератора на цилиндрическом резонаторе с использованием активных двухполюсников для последующей интеграции в ОИС СВЧ.

В цилиндрических резонаторах существуют следующие колебания: электрические – E_{mnp} и магнитные – H_{mnp}. На рис. 1 показаны структуры трёх основных типов колебаний: E_{010}, H_{111}, H_{011}.

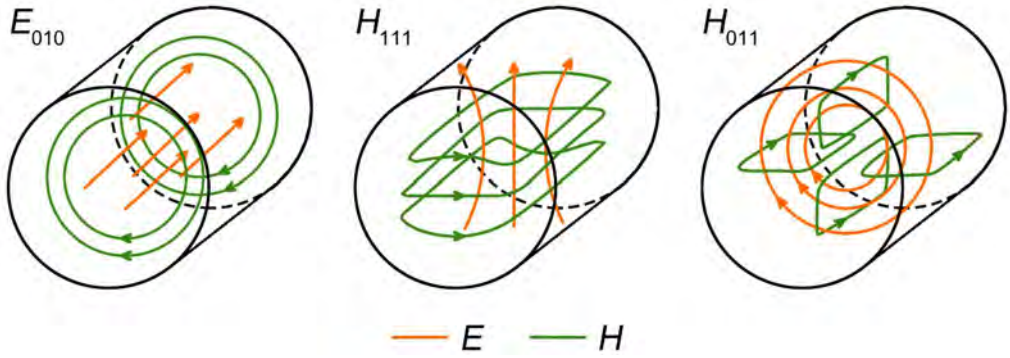


Рис. 1. Структура электромагнитного поля в цилиндрическом резонаторе для разных типов колебаний

Резонансные частоты цилиндрического резонатора вычисляются по формуле:

$$f = \frac{c}{\lambda_0},$$

где c – скорость света в вакууме,

λ_0 – резонансная длина волны.

Резонансная длина волны, в свою очередь, зависит от типа колебаний и рассчитывается по формулам [4]:

– для волн типа E_{mnp}:

$$\lambda_0 = \frac{2}{\sqrt{\left(\frac{p}{L}\right)^2 + \left(\frac{\upsilon_{mn}^E}{\pi \cdot R}\right)^2}},$$

– для волн типа H_{mnp}:

$$\lambda_0 = \frac{2}{\sqrt{\left(\frac{p}{L}\right)^2 + \left(\frac{\upsilon_{mn}^H}{\pi \cdot R}\right)^2}},$$

где υ_{mn}^E, υ_{mn}^H – корни функций Бесселя и их производных,

L – длина резонатора,

R – радиус.

Для проведения первых экспериментов из нескольких цилиндров был выбран один – с высотой 34 мм и диаметром 78 мм. Его резонансные частоты были рассчитаны и сведены в таблицу.

ТАБЛИЦА. Резонансные частоты цилиндра

L, мм	R, мм	E_{010} f, ГГц	H_{111} f, ГГц	H_{011} f, ГГц
34	39	2,944	4,954	6,44

Модель исследуемого генератора была построена в учебной версии *T-FLEX CAD* (рис. 2).

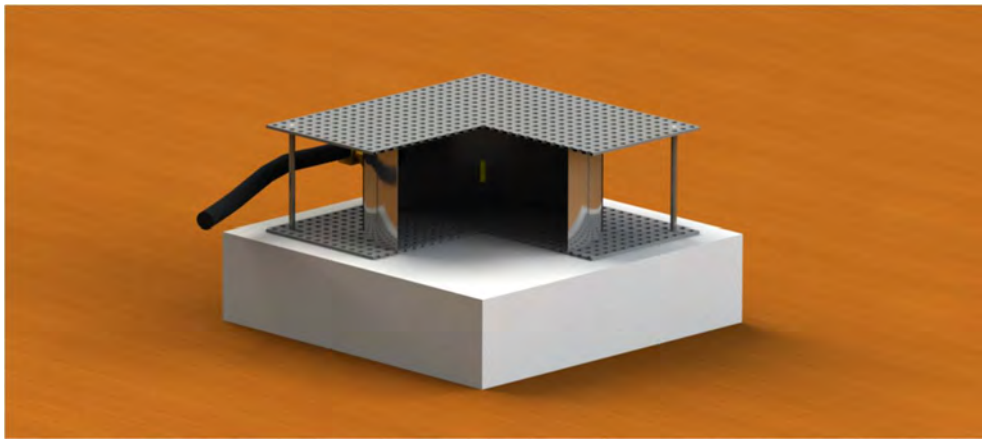


Рис. 2. 3D модель генератора

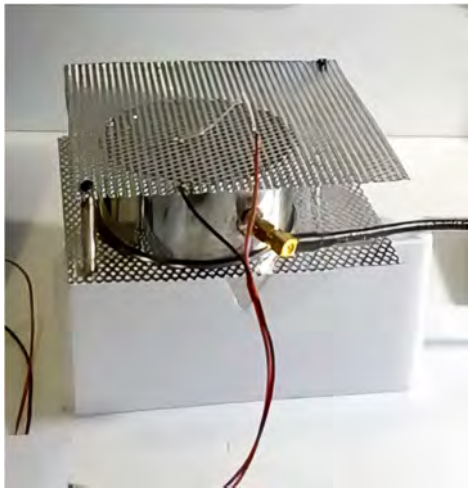


Рис. 3. Макет генератора

Далее был создан макет генератора (рис. 3) и собран стенд для проведения измерений. Генератор представляет собой металлический цилиндр, ограниченный поверхностями с перфорацией сверху и снизу, активный элемент помещается внутрь этой конструкции. Питание осуществляется с помощью проводников от регулируемого источника напряжения. Уровень генерации оценивался с помощью спектроанализатора.

После подачи напряжения на активный элемент спектроанализатор показывает следующую характеристику (рис. 4). Генерация начинается около 4 ГГц, но отсутствуют тонкие пиковые спектральные линии характерные для генератора.

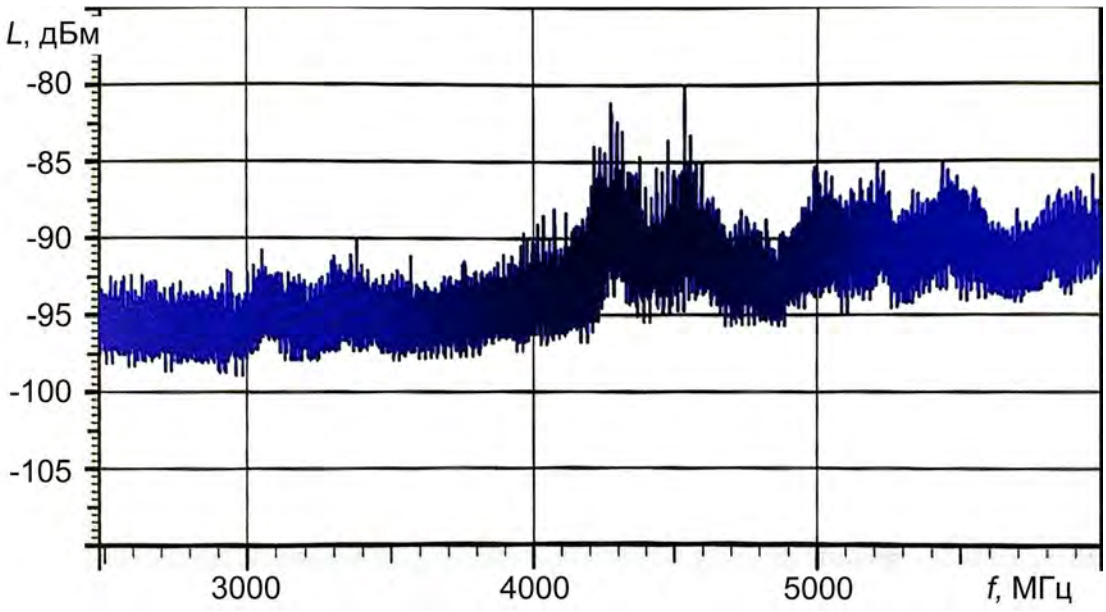


Рис. 4. Частотная характеристика

Эксперимент можно считать удачным, так как удалось запустить генератор, хотя назвать это чистой генерацией нельзя. По результатам эксперимента было решено увеличить добротность резонатора, заменив перфорированные поверхности на цельные.

На следующем этапе работ также была продумана 3D-модель устройства (рис. 5, а), после чего был собран лабораторный стенд. Реальный вид устройства представлен на рис. 5, б, в нём съём энергии происходит как с боковой поверхности, так и через нижнее основание цилиндра.

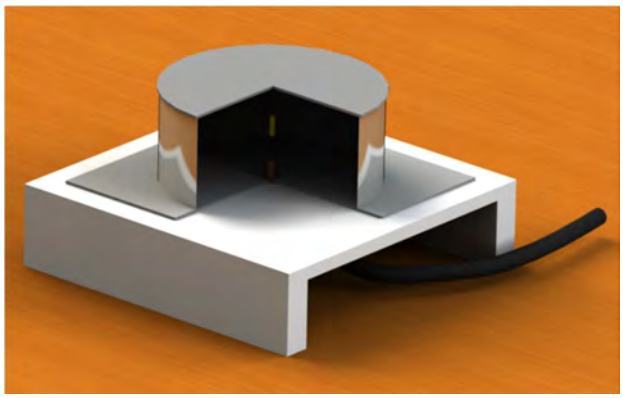
а)  б) 

Рис. 5. Генератор на цилиндрическом резонаторе: а) 3*D* модель, б) макет

Данная конструкция показала в ходе эксперимента следующую частотную характеристику (рис. 6.).

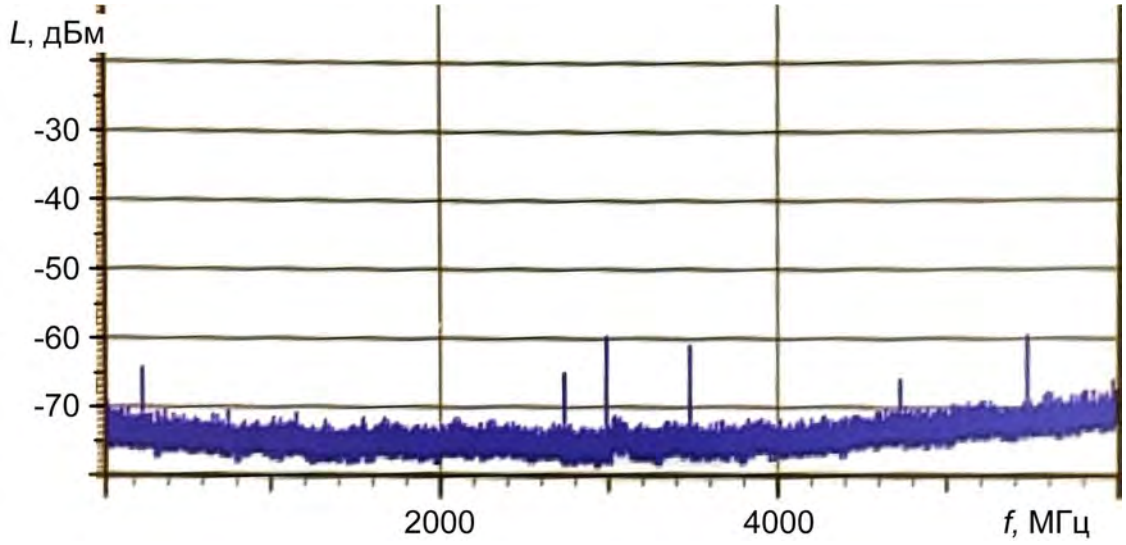


Рис. 6. Частотная характеристика

Как видно из рис. 6, была получена стабильная генерация с различимыми максимумами по мощности на частотах 2.8, 3, 3.5, 4.7 и 5.4 ГГц. Также есть генерация на частоте около 300 МГц, характер которой не исследован.

Несоответствие между теоретическими и экспериментальными данными можно объяснить меньшей добротностью реального резонатора, потерями в местах соединения боковой грани с основаниями, а также «чистотой» используемых для резонатора материалов.

Вывод: генератор на цилиндрическом резонаторе работоспособен, активный двухполюсник в виде туннельного диода способен компенсировать потери даже в объёмной конструкции. Все полученные колебания стабильны.

Список используемых источников

1. Крылов В. П. Устройство для измерения диэлектрических свойств материалов при нагреве. Пат. 2744487 Российская Федерация; заявитель и патентообладатель Акционерное общество «Обнинское научно-производственное предприятие «Технология» им. А. Г. Ромашина». – № 2020122411; заявл. 07.07.2020; опубл. 10.03.2021.

2. Алексейцев С. А. Торцевая антенна дипольного вида. Пат. 2743624 Российская Федерация; заявитель и патентообладатель Федеральное государственное бюджетное образовательное учреждение высшего образования «Новосибирский государственный технический университет». – № 2020117228; заявл. 26.05.2020; опубл. 20.02.2021.

3. Бочаров Е. И., Коновалова Е. А., Седышев Э. Ю. Исследование генератора на активном двухполюснике в сферическом резонаторе // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. Т. 3. С. 401–403.

4. Пименов Ю. В., Вольман В. И., Муравцов А. Д. Техническая электродинамика. М.: Радио и связь, 2002. 536 с.

УДК 53.08
ГРНТИ 29.03

ЭКСПЕРИМЕНТАЛЬНАЯ ПРОВЕРКА ТЕОРЕМЫ ШТЕЙНЕРА С ПОМОЩЬЮ КРУТИЛЬНОГО МАЯТНИКА

Т. Е. Кузнецова, В. Г. Урванцев, Н. Л. Урванцева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Ничто не может заменить студенту работу с реальными приборами, это первые его шаги в исследовательской деятельности. Однако, столкнувшись с дистанционным режимом работы, все стали внимательнее относиться к виртуальным работам. Очевидно, что недостаток «работы руками» необходимо компенсировать повышением внимания к теории и, в частности, к обработке результатов измерений. Представленная статья посвящена постановке виртуальной работы по проверке теоремы Штейнера.

лабораторный практикум, колебания, погрешность измерения, метод наименьших квадратов.

Концу прошлого века мы обязаны рождением виртуальных лабораторных работ. На тот момент это предоставляло уникальную возможность создания лабораторного комплекса при минимальной затрате средств. «Реальные» работы часто просто заменялись их виртуальными аналогами. Конечно, ничто не может заменить студенту работу с настоящими приборами, и это особенно важно, так как это фактически получение первых навыков эксперимента. Усовершенствование виртуального комплекса в условиях дистанционного или смешанного формата образования гарантирует высокое качество преподавания. Недостаток общения студентов с реальными приборами необходимо компенсировать повышенным вниманием к постановке задач, теоретической оценке ожидаемого результата и обработке результатов измерений.

Лабораторный практикум курса физики по разделу «Механика» университета уже содержит работу [1] по определению момента инерции диска с помощью его крутильных колебаний (1.3). В лабораторной установке горизонтально расположенный диск 1 подвешивается на проволоке 2 так, что ось вращения проходит через центр масс диска (рис. 1).

а) б)

Рис. 1. а) крутильный маятник ; б) крутильный маятник с дополнительными цилиндрами

При повороте тела в горизонтальной плоскости возникает момент сил упругости, стремящейся вернуть систему в исходное состояние. При небольших углах закручивания проволоки φ момент сил пропорционален углу поворота:

$$M_z = -D\varphi_z ,$$

где D – модуль кручения проволоки. Учитывая, что ε_z – проекция ускорения на ось z, а I_z – момент инерции тела относительно оси z и используя основное уравнение динамики вращения твердого тела вокруг неподвижной оси [2]:

$$I_z \varepsilon_z = M_z ,$$

получено уравнение колебаний крутильного маятника:

$$\varphi_z'' + \frac{D}{I}\varphi_z = 0 . \qquad (1)$$

Период колебаний такой системы равен:

$$T = 2\pi\sqrt{\frac{I}{D}} . \qquad (2)$$

Для определения модуля кручения D на диск маятника симметрично относительно оси укрепляется два одинаковых цилиндрических груза (рис. 1, б). Известно, что момент инерции – величина аддитивная, то есть момент инерции в последнем случае равен :

$$I + I_1,$$

где I_1 – момент инерции цилиндров. А период колебаний системы – $T_1 = 2\pi\sqrt{\frac{I + I_1}{D}}$. Измерив периоды колебаний T и T_1, можно исключить величину D из определения момента инерции диска:

$$I = I_1 \frac{T^2}{T_1^2 - T^2}.$$

Эта же лабораторная установка позволяет проверить теорему Штейнера изменяя расстояния цилиндров от оси вращения (работа 1.4. [1]).

В предлагаемой работе несколько другим способом решается та же задача проверка теоремы Штейнера (рис. 2).

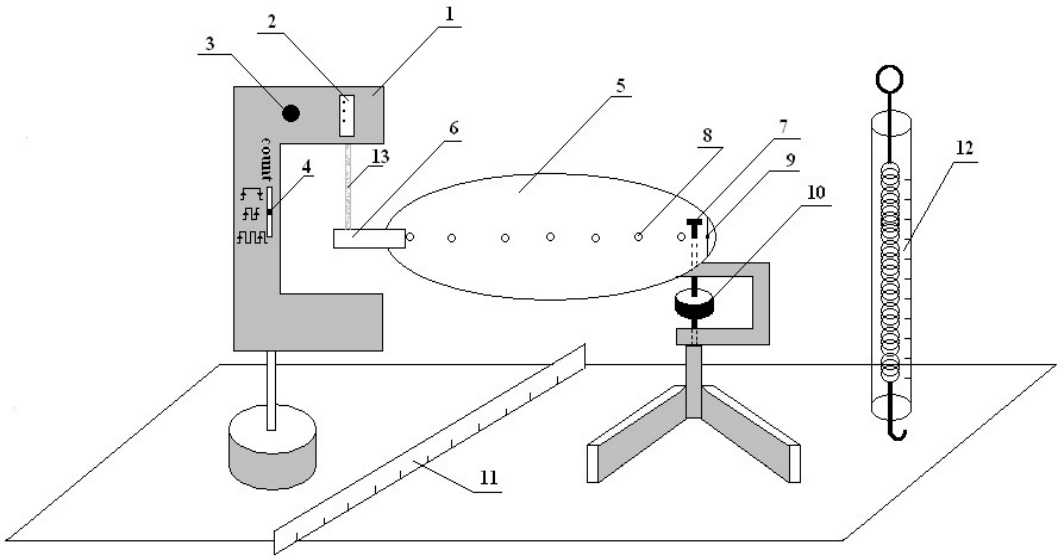


Рис. 2. Схема экспериментальной установки

Ось диска 5 связана с плоской спиральной металлической пружиной 10. Поворот диска из положения равновесия приводит к возникновению момента упругих сил, возвращающих диск в исходное состояние. Согласно закону Гука, этот момент сил пропорционален углу поворота стальной пружины маятника (аналогично тому, как это было в случае диска, подвешенного на проволоке). Здесь *D* (упругую константу пружины). называют коэффициентом восстановления. Уравнение колебаний в этом случае будет точно таким же (1). И момент инерции также определяется по результатам измерения периода колебаний маятника (2). Однако в представленном эксперименте можно непосредственно измерить упругую константу *D*. С этой целью проводятся измерения зависимости момента сил упругих сил M_z

от угла закручивания пружины φ. Для определения момента возвращающих сил, действующих на пружину, используется динамометр 12, крючок которого вставляется в отверстие 9. Момент сил, создаваемый динамометром, позволяет уравновесить возвращающий момент, возникающий в плоской спиральной пружине при повороте диска на заданный угол. Сила, действующая со стороны динамометра, измеряется несколько раз. Динамометр должен быть расположен перпендикулярно диаметру диска. Плечо силы – расстояние между точкой 9 и осью вращения диска измеряется с помощью линейки. Находится средний для заданного угла φ момент силы $\overline{M}$. Для определения числа измерений момента силы необходимо оценить систематическую погрешность измерений. В нашем случае систематическая погрешность зависит от погрешности измерения силы и погрешности измерения плеча силы. Вычисляем относительную погрешность $\delta M = \sqrt{\left(\frac{\Delta F}{F}\right)^2 + \left(\frac{\Delta l}{l}\right)^2}$ и определяем систематическую погрешность:

$$\Delta M_{\text{сист}} = \overline{M}\delta M \ .$$

Известно, полная погрешность измерения определяется как систематической так и случайной погрешностью:

$$\Delta M = \sqrt{\left(\Delta M_{\text{сист}}\right)^2 + \left(\Delta M_{\alpha}\right)^2} \ .$$

Случайная погрешность (запишем ее для измеряемой величины M):

$$\left(\Delta M\right)_{\text{случ}} = t\left(\alpha, n\right)\sigma_{\overline{M}} ,$$

где α – доверительная вероятность (в лабораторных работах обыкновенно используется $\alpha = 0{,}68$),

$t\left(\alpha, n\right)$ – коэффициент Стьюдента (зависит от доверительной вероятности α и числа опытов n),

$\sigma_{\overline{M}}$ – среднее квадратичное отклонение среднего значения измеряемой величины M. Среднее квадратичное отклонение отдельного измерения $\sigma_M = \sqrt{\frac{\sum (M_i - \overline{M})^2}{n-1}}$ рассчитывается по [3] результатам предварительных измерений. Среднюю квадратичную погрешность среднего можно уменьшить увеличивая число измерений n :

$$\sigma_{\overline{M}} = \sqrt{\frac{\sum_{i=1}^{n}\left(M_i - \overline{M}\right)^2}{n\left(n-1\right)}}.$$

Уменьшать случайную ошибку целесообразно до тех пор, пока общая погрешность не будет полностью определяться погрешностью измерительных приборов. Это условие можно считать выполненным, если $\Delta M \le \frac{\Delta M_{\text{сист}}}{10}$ [3]. Практически обычно можно удовлетвориться значительно менее жестким условием $\Delta M \le \frac{\Delta M_{\text{сист}}}{2}$.

$$\left(\Delta M\right)_{\text{случ}} = t\left(\alpha, n\right)\sigma_{\overline{M}} = \frac{t\left(\alpha, n\right)\sigma_M}{\sqrt{n}} \approx \frac{\Delta M_{\text{сист}}}{2}.$$

Число измерений $n = \left(\frac{2t_{\alpha n}\sigma_M}{\Delta M_{\text{сист}}}\right)^2$. В нашем случае $n = 6$. При данном φ момент сил определяется 6 раз. Сила, действующая со стороны динамометра, измеряется 6 раз (три раза при повороте диска по часовой стрелке и три раза при повороте диска против часовой стрелки). Находится средний для заданного угла φ момент силы $\overline{M}$. Результат усреднения изображается точкой на графике, изображающем зависимость момента сил M_z, действующих на спиральную пружину, от угла ее закручивания φ (каждая точка графика является результатом усреднения экспериментальных результатов). Очевидно, что угол наклона графика – это модуль *D*. Эксперимент показал, что при углах закручивания от 0 до 3π пружина сохраняет свои упругие свойства (линейность зависимости была проверена методом наименьших квадратов [4]). Величина коэффициента восстановления *D* с вероятностью $\alpha = 0,68$ равна:

$$D = 0,0222 \pm 0,0013 Н \cdot м / рад.$$

Согласно теореме Штейнера момент инерции *I* относительно произвольной оси *z* равен моменту инерции I_c относительно оси z_c, параллельной данной и проходящей через центр масс тела, плюс произведение массы *m* тела на квадрат расстояния *d*:

$$I = I_c + md^2 .$$

Момент инерции является линейной функцией от d^2. Как было показано ранее, момент инерции можно найти измерив период колебаний :

$$I = \frac{DT^2}{4\pi^2} .$$

Для проверки теоремы Штейнера также используем метод наименьших квадратов. При заданном угле закручивания $\varphi = 2\pi$ и заданном положении оси многократно измеряется время 10 колебаний. и находится средняя величина периода $\overline{T}$ и средняя величина момента инерции $\overline{I}_i$ для данного положения оси (данного *d*). Эксперименты проводятся для 4 различных положений оси. В результате опытов получают пары чисел $(0,\overline{I}_1);(d,\overline{I}_2);(2d,\overline{I}_3);(3d,\overline{I}_4)$ и строится график $\overline{I}(d^2)$. Студенты убеждаются в том, что эта зависимость близка к линейной. Предполагая, что величины d_i измерены без ошибок, а величины I_i могут содержать случайные ошибки, предлагается построить оценку функции регрессии [4] $\tilde{I}(d^2)$ – функцию условного математического ожидания момента инерции диска $\tilde{I}$ от квадрата расстояния d оси от центра масс диска. Строится функция регрессии: $\tilde{I} = \tilde{a}d^2 + \tilde{b}$ и ищутся оценки неизвестных параметров $\tilde{a}$ и $\tilde{b}$. В качестве параметров естественно взять такие, при которых прямая $\tilde{I} = \tilde{a}d^2 + \tilde{b}$ ближе всего подходит к экспериментальным точкам. Роль меры отклонений играет сумма квадратов разностей: $S = \sum_{i=1}^{n=4}\left(I_i - \tilde{b} - \tilde{a}d_i^2\right)^2$. Тогда оценками $\tilde{a}$ и $\tilde{b}$ будут служить такие значения, при которых эта сумма принимает наименьшее значение. С этой целью рассматриваем *S* как функцию $\tilde{a}$ и $\tilde{b}$ и записываем условие ее экстремума $\frac{\partial S}{\partial \tilde{a}} = 0; \frac{\partial S}{\partial \tilde{b}} = 0$. Дифференцируя *S* и введя обозначения:

$$S_1 = \sum_n d_i^2; S_2 = \sum_n d_i^4; V_0 = \sum_n I_i; V_1 = \sum_n d_i^2 I_i ,$$

получаем систему уравнений для определения $\tilde{a}$ и $\tilde{b}$:

$$\begin{aligned} S_1\tilde{a} + n\tilde{b} &= V_0 \\ S_2\tilde{a} + S_1\tilde{b} &= V_1 \end{aligned} .$$

Решение системы позволяет определить оценки параметров:

$$\tilde{a} = \frac{S_1 V_0 - n V_1}{\Delta}; \tilde{b} = \frac{S_1 V_1 - S_2 V_0}{\Delta},$$

здесь Δ – определитель системы $\Delta = S_1^2 - S_2 n$.

Расчеты показали, что $\tilde{a} = 0,225 \pm 0,005$кг, а $\tilde{b} = (2 \pm 1) 10^{-3}$ кг $\cdot$ м^2. Полученные данные хорошо согласуются с результатами расчета с помощью теоремы Штейнера.

Список используемых источников:

1. Жуков В. М., Князев С. А., Костин А. А., Кузьмина М. П., Постникова Л. А., Широчин Л. А. Физика. Механика: Методические указания к лабораторным работам / СПбГУТ. СПб., 2005.

2. Савельев И. В. Курс общей физики: учебное пособие. В 3-х т. Т. 1. Механика. Молекулярная физика. СПб.: Лань, 2011. 432 с. ил. (учебники для вузов. Специальная литература.). ISBN 978-58114-1207-5.

3. Зайдель А. Н. Элементарные оценки ошибок измерений. Л.: Наука, Ленинградское отд., 1967. 88 с.

4. Азизов А. М., Курицин А. Г., Никитенко В. Г. Основы прикладной математики. Теория вероятностей и математическая статистика. СПб.: Химия, 1994. 264 с. ISBN 5-7245-1004-9.

УДК 621.375
ГРНТИ 47.45

ИССЛЕДОВАНИЕ ПОДАВЛЕНИЯ ИСКАЖЕНИЙ МЕТОДОМ ДВОЙНОЙ ОБРАТНОЙ СВЯЗИ

А. Э. Ланда, Е. Ю. Ларьков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Экспериментально исследован новый метод линеаризации нелинейного усилителя двойной обратной связью. Линеаризация достигается благодаря комбинации двух колец обратной связи (кольцо отрицательной обратной связи и кольцо положительной обратной связи), в которые включен вспомогательный усилитель. В ходе исследования была экспериментально проверена новая методика оценки подавления шумов устройством линеаризации.

экспериментальный метод исследования, линеаризации нелинейного усилителя СВЧ-диапазона, двойная обратная связь, подавление шумов.

С развитием современных телекоммуникационных технологий возникает значительная потребность в усилительных устройствах СВЧ-диапазона, обладающих высоким КПД и малым уровнем интермодуляционных искажений. Одним из возможных решений данной проблемы является разработка новых методов линеаризации нелинейных усилителей.

На данный момент широкое применение нашли следующие методы линеаризации нелинейных усилителей: внесения предискажений (*predistortion linearization*), отрицательной обратной связи (*feedback linearization*), компенсационный (*feedforward linearisation*) [1, 2, 3]. Компенсационный метод позволяет добиться наибольшей глубины подавления интермодуляционных искажений, однако этот метод требует очень высокой точности выполнения. Кроме того, усилительные устройства, созданные на его основе, в ряде случаев проигрывают по КПД другим вариантам построения усилителей [4, 5]. В данной статье отражены результаты предварительного экспериментального исследования метода линеаризации двойной обратной связью, который позволяет обеспечить высокий уровень подавления интермодуляционных искажений без значительного снижения КПД устройства [6].

Рассмотрим работу устройства, изображенного на рис. 1 при подаче на его вход одночастотного сигнала, вида: $E_0 \cos \omega t$. Устройство представляет нелинейный усилитель мощности (УМ) с кольцом положительной обратной связи на входе (кольцо ПОС), охваченный отрицательной обратной связью (кольцо ООС).

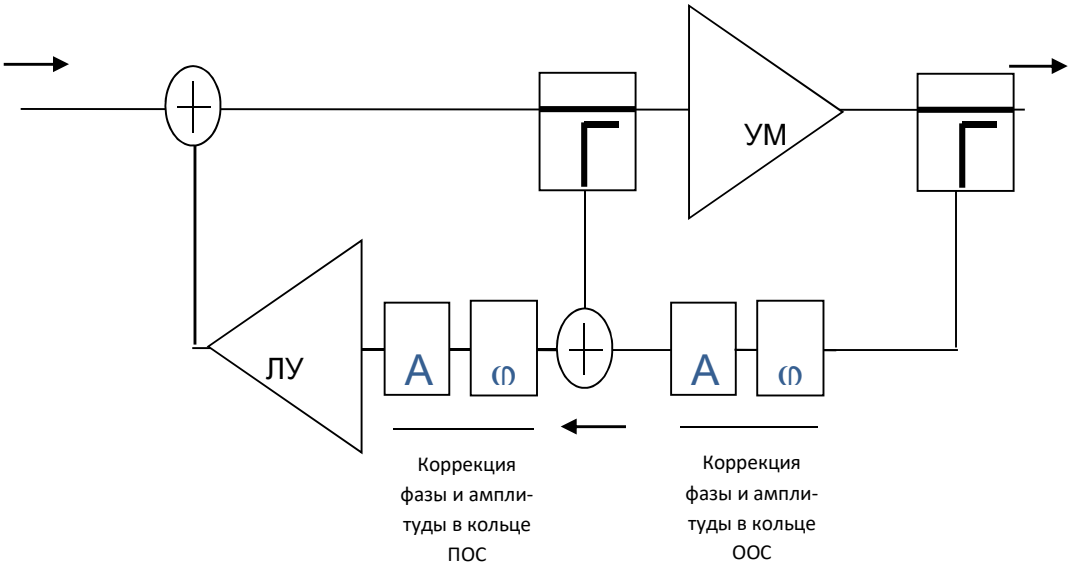


Рис. 1. Блок-схема устройства линеаризации усилителя СВЧ-диапазона методом двойной обратной связи

В кольцо положительной обратной связи включен линейный усилитель (ЛУ). Обозначим суммарный передаточный коэффициент (с учетом

фазового набега) всех элементов кольца ПОС – $a_1 e^{-j\varphi_1(f)} = \dot{a}_1$. Передаточный коэффициент всех элементов кольца ООС, кроме нелинейного усилителя мощности, обозначим – $a_2 e^{-j\varphi_2(f)} = \dot{a}_2$.

Передаточный коэффициент нелинейного усилителя мощности – $K_{PA}(U_1)e^{-j\varphi_{PA}(f,U_1)} = \dot{K}_{PA}(U_1)$, где U_1 – амплитуда напряжения на входе усилителя. Используя метод комплексных амплитуд, несложно определить напряжение на выходе устройства:

$$\dot{U}_{out} = \frac{\dot{a}_3 \dot{K}_{PA}(U_1) E_0}{1 - \dot{a}_1 - \dot{a}_2 \dot{K}_{PA}(U_1)}.$$

Допустим, на частоте f_0 $\dot{a}_1 = 1$, $1 - \dot{a}_1 = 0$, а $\mathrm{Re}(\dot{a}_2 \dot{K}_{PA}(U_1)) < 0$. В этом случае:

$$\dot{U}_{out} = -\frac{\dot{a}_3 E_0}{\dot{a}_2},$$

а передаточный коэффициент устройства линеаризации:

$$\dot{K} = \frac{\dot{U}_{out}}{E_0} = -\frac{\dot{a}_3}{\dot{a}_2}.$$

Таким образом, в случае точного выполнения условия $1 - \dot{a}_1 = 0$ выходной сигнал на частоте f_0 не будет зависеть от нелинейного усилителя мощности, а это значит, что будут полностью подавлены вносимые этим усилителем шумы и искажения. Более подробный анализ, проведенный в работе [7], показал, что двойная обратная связь подавляет вносимые усилителем мощности шумы, так же как двойная обратная связь подавляет интермодуляционные искажения. При идеальной настройке двойной обратной связи шумы и искажения, вносимые основным усилителем, будут подавлены полностью (в этом случае выходные шумы всего устройства будут определяться шумами вспомогательного усилителя, который поэтому необходимо выбирать малошумящим). Разумеется, абсолютно точное выполнение условий линеаризации является абстракцией (к тому же возможной, даже в теории, только на одной частоте), но достаточно точная настройка колец обратной связи может позволить добиться глубокого подавления интермодуляционных искажений и шумов в достаточно широкой полосе частот [7].

Экспериментальная оценка шумов и линеаризации (т. е. подавления интермодуляционных искажений) требует наличия специализированного

оборудования, недоступного на данном этапе исследования. Для возможности экспериментально исследовать подавление вносимых усилителем искажений, было принято решение ввести искусственный источник помех на выход устройства, и оценить подавление с помощью обычного осциллографа. Для проверки предложенного метода был собран экспериментальный макет (рис. 2).

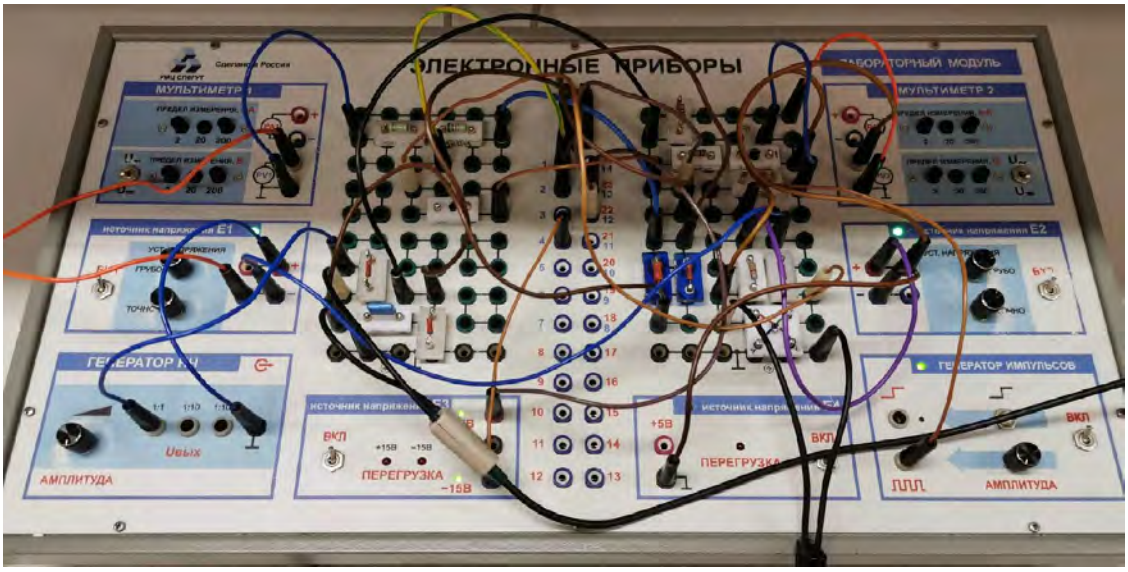


Рис. 2. Экспериментальный макет усилительного устройства

Эквивалентная принципиальная схема устройства представлена на рис. 3. На схеме инвертирующий усилитель на операционном усилителе служит как вспомогательный (линейный) усилитель, а усилительный каскад на полевом транзисторе, выполняет функцию нелинейного усилителя мощности. В схему введен G2 – генератор помехи в виде прямоугольных импульсов. По подавлению этих импульсов двойной обратной связью можно оценить подавление шумов и искажений на выходе устройства.

В экспериментальном макете, в качестве нелинейного усилителя был использован неинвертирующий усилительный каскад, реализованный на операционном усилителе КР140УД20А.

Данный усилительный каскад был охвачен двойной обратной связью с включенным в цепь ОС линейным усилителем, реализованным на полевом транзисторе. В качестве источника помехи к цепи ОС был подключен генератор прямоугольных импульсов.

При подключении цепи ОС (цепи отрицательной ОС идущей от резистора R10 ко входу, и цепи положительной ОС идущей с выхода операционного усилителя на вход) сигнал помехи подавляется (рис. 4).

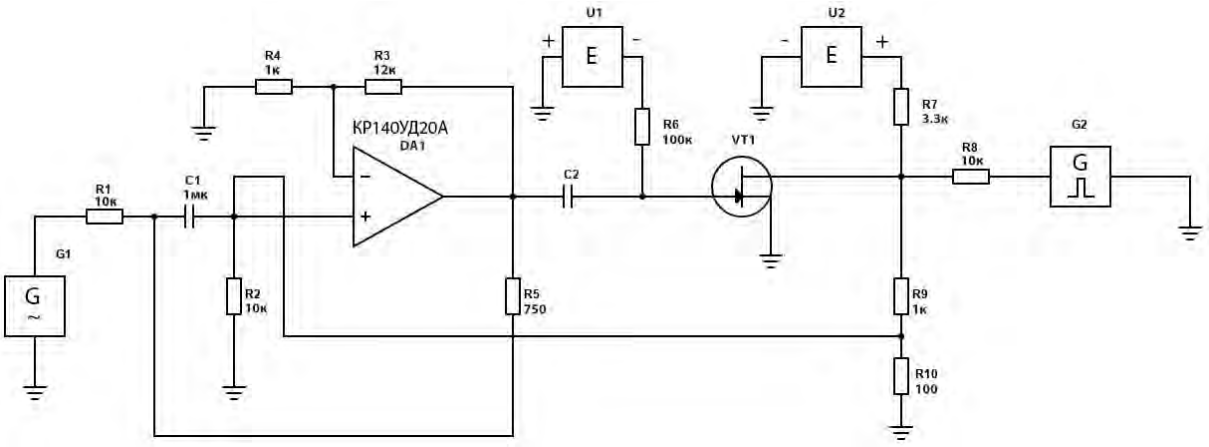


Рис. 3. Принципиальная схема устройства

Рис. 4. Сигнал помехи с включенной цепью ОС (слева) и с выключенной цепью ОС (справа). Масштаб на экране осциллографа одинаковый

Несмотря на то что собранный макет реализует метод двойной обратной связи крайне неточно (необходимая точная настройка кольца положительной обратной связи пока не осуществлена), эксперимент показал подавление вносимых искажений примерно в 3 раза по напряжению и, соответственно, примерно в 9 раз по мощности. Малая глубина подавления искажений объясняется низкой точностью при реализации обратных связей.

Проведенное экспериментальное исследование показывает, что без использования спектроанализатора возможно оценить линеаризацию и подавление шумов усилительного устройства, охваченного двойной ОС.

Список используемых источников

1. Kumar S. Power amplifier linearization using MMICs // Microwave journal. 1992 April. Pp. 96–104.

2. Perez F. Ballesteros E. Perez J. Linearisation of microwave power amplifier using active feedback networks // Electronic letters. 1985, V. 21, № 1. Pp. 9–10.

3. Raab F. H., Asbeck P. M., Cripps S., Kenington P. B., Popovic Z. B., Pothecary N., Sevic J. F., Sokal N. O. RF and Microwave Power Amplifier and Transmitter Technologies – Part 4 // High Frequency Electronics November 2003. Pp. 38–49.

4. Eid E. E., Channouhi F. M., Beuregard F. Optimal feedforward linearization system design // Microwave journal. 1995 November. Pp. 78–86.

5. Kenington P. B. Efficiency of feedforward amplifiers // IEE procedurings. 1992. V. 139. № 5. Pp. 591–593.

6. Иванов О. А., Корнилов С. А., Овчинников К. Д. Линеаризация амплитудной характеристики СВЧ-усилителей мощности методом комплексной обратной связи // Труды учебных заведений связи 1996. № 161. С. 88–93.

7. Ланда А. Э. Энергетически эффективный метод линеаризации активной обратной связью транзисторного усилителя мощности СВЧ диапазона: дис. ... канд. техн. наук: 05.12.07. СПб., 2005. 125 с.

УДК 621.372.414
ГРНТИ 47.45.99

ПЕРЕСТРАИВАЕМОЕ ЧАСТОТНО-РАЗДЕЛИТЕЛЬНОЕ УСТРОЙСТВО НА ПОДЛОЖКЕ ИЗ ФЕРРОШПИНЕЛИ

А. Э. Ланда, Л. Р. Мугу

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе была предпринята попытка исследовать возможность создания перестраиваемого фильтра на феррошпинели. В СВЧ электронике существует потребность в перестраиваемых фильтрах, и создание фильтров на ферритовой подложке, управляемых магнитным полем, могло бы способствовать решению этой задачи.

СВЧ, резонатор, фильтры СВЧ, ферритовая подложка, феррошпинель.

Перестраиваемые резонаторы на феррошпинелевой подложке (которые могут быть частью фильтра) исследовались ранее в работах, в которых была показана возможность создания резонатора с использованием ферритов. Данная статья является развитием указанных работ, где рассматривался вопрос об использовании подложки из феррошпинели [1, 2, 3, 4, 5].

В рамках данной работы была поставлена задача исследовать возможность построения перестраиваемого фильтра на феррошпинели.

Первоначально был выбран вариант шлейфного фильтра на микрополосковой линии, показанный на рис. 1.

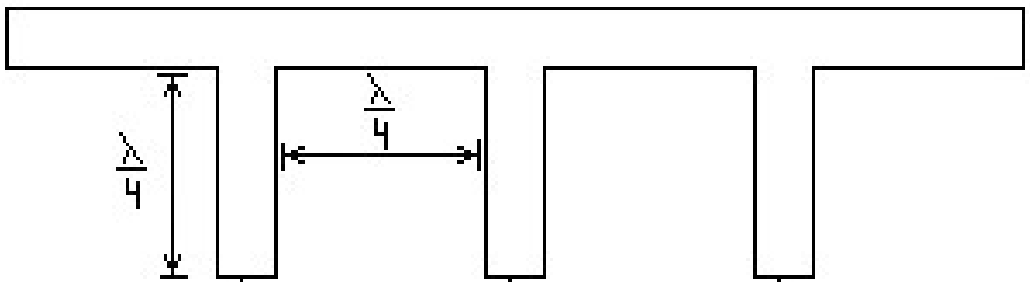


Рис. 1. Схемотехническое строение фильтра

Как было ранее показано, феррошпинель позволяла создавать перестраиваемое частотно-разделительное устройство [4]. Поскольку у феррошпинели магнитная проницаемость заметно отличается от единицы и зависит от магнитного поля, приложенного к феррошпинели, то существует возможность, меняя магнитное поле, перестраивать электрическую длину всех элементов фильтра, и, таким образом, менять АЧХ фильтра. Как известно, в обычных диэлектриках магнитная проницаемость примерно равна 1, поэтому при расчетах не учитывается, но ферриты составляют особый класс тел, у которых магнитная проницаемость может быть много больше единицы, и, следовательно, ее необходимо принимать в расчет [1, 2, 3]. В этом случае формулы для расчета имеют следующий вид:

– Скорость распространения волн в диэлектрике:

$$v = \frac{c}{\sqrt{\varepsilon_{эфф} * \mu_{эфф}}},$$

где c – скорость света,
$\varepsilon_{эфф}$ – эффективная диэлектрическая проницаемость,
$\mu_{эфф}$ – эффективная магнитная проницаемость,
v – скорость распространения волн в диэлектрике.

– Волновое сопротивление МПЛ:

$$Z_0 = 56 * \lg\left(10{,}4 * \frac{h}{W}\right) * \sqrt{\frac{\mu_{эфф}}{\varepsilon_{эфф}}},$$

где Z_0 – волновое сопротивление МПЛ,
h – высота диэлектрической подложки,
W – ширина токонесущего полоска,
$\varepsilon_{эфф}$ – эффективная диэлектрическая проницаемость,
$\mu_{эфф}$ – эффективная магнитная проницаемость,
v – скорость распространения волн в диэлектрике.

– Электрическая длина элементов фильтра:

$$\theta = \frac{l * \sqrt{\varepsilon * \mu}}{\lambda},$$

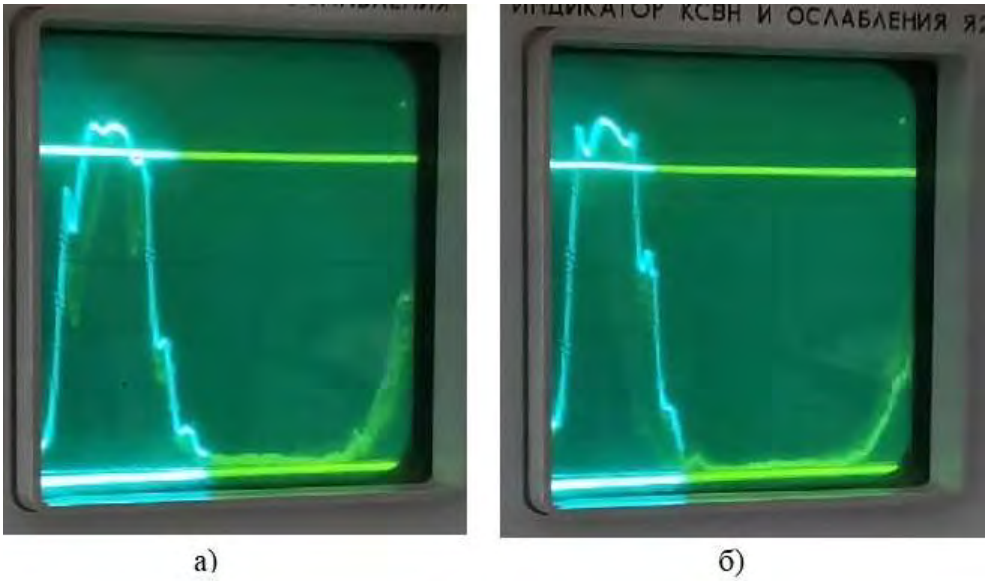
где θ – электрическая длина элементов фильтра,
l – длина элемента,
ε – диэлектрическая проницаемость,
μ – магнитная проницаемость,
λ – длина волны в вакууме.

Как можно видеть из приведенных формул, меняется как электрическая длина, так и волновое сопротивление. Но расчеты показали, что при сравнительно небольшом изменении магнитного поля можно заметно сдвинуть центральную частоту фильтра без разрушения его АЧХ, так как волновое сопротивление меняется незначительно.

Для экспериментальной проверки возможности создания перестраиваемого фильтра, был изготовлен макет на феррошпинели, магнитное поле в котором предполагалось менять с помощью постоянного магнита, перемещаемого относительно самого макета (рис. 2). Эксперимент проводился на индикаторе КСВН и ослабления Я2Р-67.

Рис. 2. Макет перестраиваемого фильтра на феррошпинели

Экспериментальные исследования передаточной характеристик исследуемого устройства (при разных положениях магнита относительно макета) показаны на рис. 3.



а) б)

Рис. 3. Смещение АЧХ фильтра при изменении положения магнита относительно макета

Измерения были проведены в диапазоне частот от 3,48 до 3,68 ГГц.

Как видно, удалось получить управляемую магнитным полем АЧХ, но не удалось добиться точного сохранения формы фильтровой характеристики. Причинами этого послужили с одной стороны неоднородность магнитного (создать однородное магнитное поле, которое одинаково действовало бы на все части фильтра, не удалось), с другой стороны сказалась неточность выполнения самого фильтра.

В дальнейшем предполагается исследовать изменение АЧХ экспериментального макета, помещенного в однородное магнитное поле. Также, предполагается попробовать создать перестраиваемый фильтр на феррошпинели со связанными линиями, который показан на рис. 4.

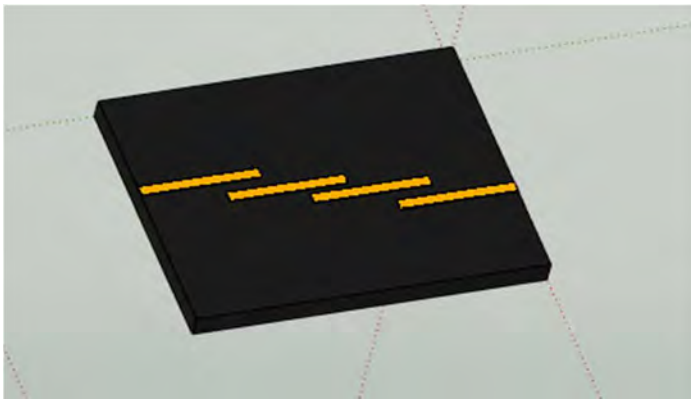


Рис. 4. Перестраиваемый фильтр на феррошпинели со связанными линиями

Список используемых источников

1. Малков Н. А. Гиротропные среды в технике СВЧ: учеб. пособие / под ред. З. Г. Черновой. Тамбов : Изд-во Тамб. гос. техн. ун-та, 2005. 104 с.

2. Fuller A. J. B. Ferrites at microwave frequencies. IET, 1987. № 23.

3. Riches E. E. Ferrites; a Review of Materials and Applications. Mills & Boon, 1972.

4. Хафизов Р. С. Управляемые частотно-разделительные устройства СВЧ диапазона на ферритах: дис. … магистра: 11.04.02 / Хафизов Руслан Сергеевич. Санкт-Петербург, 2020. 48 с.

5. Ланда А. Э., Мугу Л. Р. Полосковый резонатор СВЧ диапазона с использованием ферритовых вставок // 74-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2020» : сб. науч. ст. Спец. вып. СПб. : СПбГУТ, 2020. С. 70–72.

УДК 537.876.42
ГРНТИ 47.59.34

СИНТЕЗ МИКРОВОЛНОВОГО СУММАТОРА С ВВОДОМ/ВЫВОДОМ ЭНЕРГИИ В РАЗНЫХ СЛОЯХ ОИС СВЧ

А. С. Леонтьев, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа посвящена вопросам проектирования объёмных интегральных схем СВЧ, рассматриваются проектирование и макетирование устройства деления мощности, построенного на полосковых линиях. Интерфейсы предложенного сумматора расположены в разных слоях ОИС СВЧ. Синтезированы отдельные узлы сумматора и устройство в целом. Проведён эксперимент, описаны особенности функционирования макетов в нижней части СВЧ диапазона. Сделаны выводы о работоспособности исследуемого устройства деления мощности.

СВЧ, делитель мощности, сумматор, симметричная полосковая линия, микрополосковая линия, полосковая линия, ослабление, волновое сопротивление, ДПЛ, ТПЛ, ИПЛ.

Данная работа является продолжением работы [1], в которой рассматривается возможность создания устройств распределения мощности между слоями ОИС СВЧ за счёт одновременного использования нескольких модифицированных линий передач. Результатом этой работы является доказательство возможности деления энергии в объёме интегральной схемы СВЧ.

Предлагаемая структура СВЧ-перехода представляет собой СПЛ разделённую на две МПЛ, расположенные в разных плоскостях. Центральная пластина СПЛ вырождается в «земляную» общую пластину для МПЛ, а «земляные» пластины СПЛ переходят в токонесущие пластины МПЛ. Созданная структура делит поле с помощью такой геометрии на две части. Таким образом, предлагается ОИС делителя (сумматора) микроволнового диапазона. Величина ослабления на каждом из выводов такого делителя ожидается на уровне –3 дБ.

Для расчётов волновых сопротивлений СПЛ и МПЛ линий используются [2] и [3]. В рассмотренной конструкции используются несколько переходных устройств, которые требуют подробного расчёта и анализа. Для упрощения расчётов этих устройств была выбрана модель экспоненциального плавного перехода (рис. 1), описанная в [4]. Согласно источнику [4], «экспоненциальным считается переход, у которого волновое сопротивление изменяется вдоль координаты «*x*» по экспоненциальному закону»:

$$\rho(x) = \rho(0) \cdot e^{\alpha x},$$

где α – постоянная;

$\rho(0)$ – волновое сопротивление в начале координат.

Если принять, что постоянная распространения $\gamma(x) = \gamma = const$, то закон изменения волнового сопротивления примет вид:

$$\rho(x) = \rho(0) \cdot e^{\ln(R)\frac{x}{l}},$$

где $\ln(R)$ – коэффициент формы кривой волнового сопротивления.

На первом этапе исследования были рассмотрены варианты коммутации СПЛ и МПЛ без использования промежуточных типов линий передач. За основу было взято предположение, что волна поровну делится между слоями СПЛ, разделёнными центральной пластиной, поэтому исследования проводились на НПЛ. По сути рассматривается инвертированная НПЛ (ИПЛ), у которой верхняя и нижняя пластины на одном конце линии меняют свои топологии таким образом, что линия преобразуется в такую же перевернутую НПЛ на втором конце. Важно отметить, что сигнал, прошедший через любую ИПЛ инвертируется, так как на выходе устройства присутствует перевернутая волна по сравнению со входом.

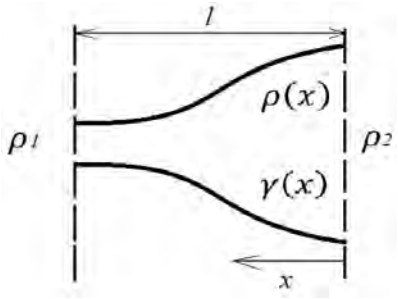


Рис. 1. Плавный переход

Самый простой случай такой линии – пластины треугольной формы на разных слоях ОИС, их расположение показано на рис. 2. Масштабный макет исследован в диапазоне 50–1 500 МГц.

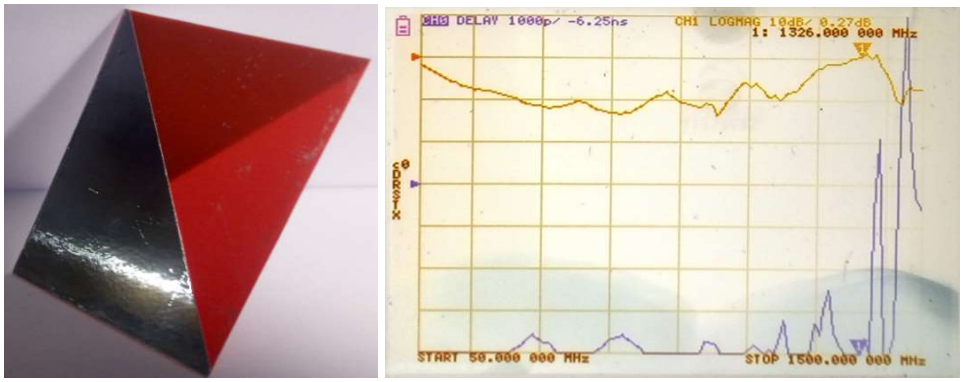


Рис. 2. Исследование ИПЛ треугольной формы

Средняя величина ослабления такого перехода зафиксирована на уровне –10 дБ, однако в диапазоне 1 100–1 400 МГц величина ослабления

не достигает –1 дБ. Стоит отметить, что использование грубых переходных конструкций негативно сказывается на характеристике ослабления.

Также был собран макет ИПЛ, у которой топология слоёв близка к U-образной форме (рис. 3).

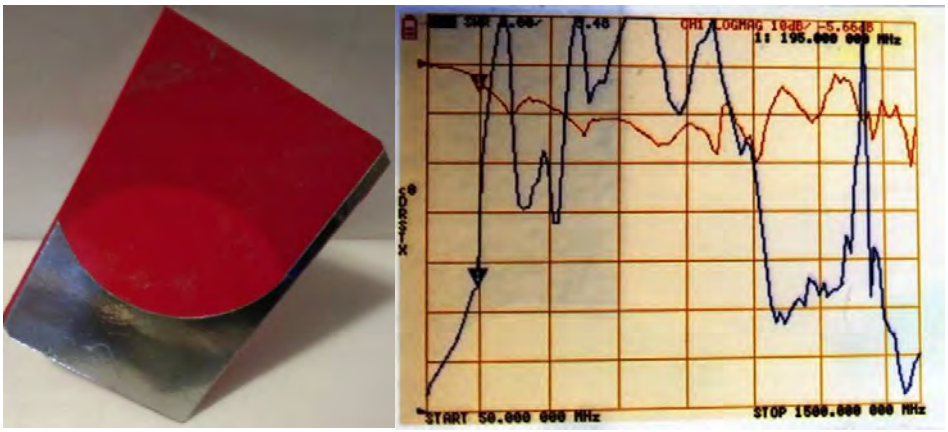


Рис. 3. Исследование ИПЛ U - образной формы

Общая характеристика ослабления такой ИПЛ схожа с характеристикой ИПЛ треугольной формы, но в характеристике второго макета явно прослеживается влияние резонансного контура, образованного паразитными параметрами перехода.

Эксперимент показывает, что конструкция синтезируемого делителя должна содержать промежуточные переходные линии. Наиболее близкой линией схожей топологии с СПЛ и НПЛ является трёхпроводная полосковая линия (ТПЛ). Используя методику расчёта модифицированных типов линий, описанную в [5], легко перейти от ТПЛ к двухпроводной полосковой линии (ДПЛ), которую легко согласовать с МПЛ.

Для проверки промежуточных результатов был собран и исследован макет ДПЛ, результаты эксперимента представлены на рис. 4. Величина ослабления зафиксирована на уровне –0,5 дБ в диапазоне 2–4 ГГц.

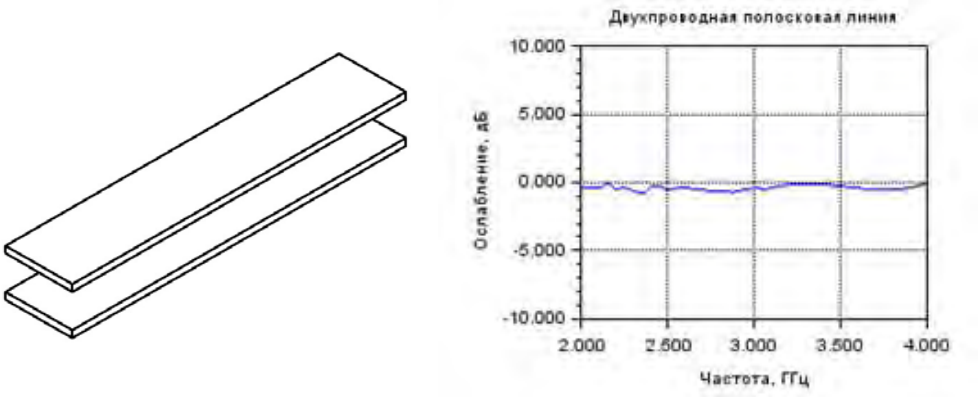


Рис. 4. Характеристика ослабления двухпроводной полосковой линии

Поскольку трёхпроводная полосковая линия, состоящая из двух двухпроводных полосковых линий, является лишь переходной конструкцией, её также необходимо согласовать с МПЛ. Был собран и исследован макет перехода между МПЛ и ДПЛ. Рассматривалось ослабление волны при прохождении в противоположных направлениях. Результаты эксперимента представлены на рис. 5. Характеристики ослабления при прохождении энергии в противоположных направлениях не совпадают, что свидетельствует о неудачном выборе топологии перехода. В среднем величина ослабления зафиксирована на уровне –5 дБ.

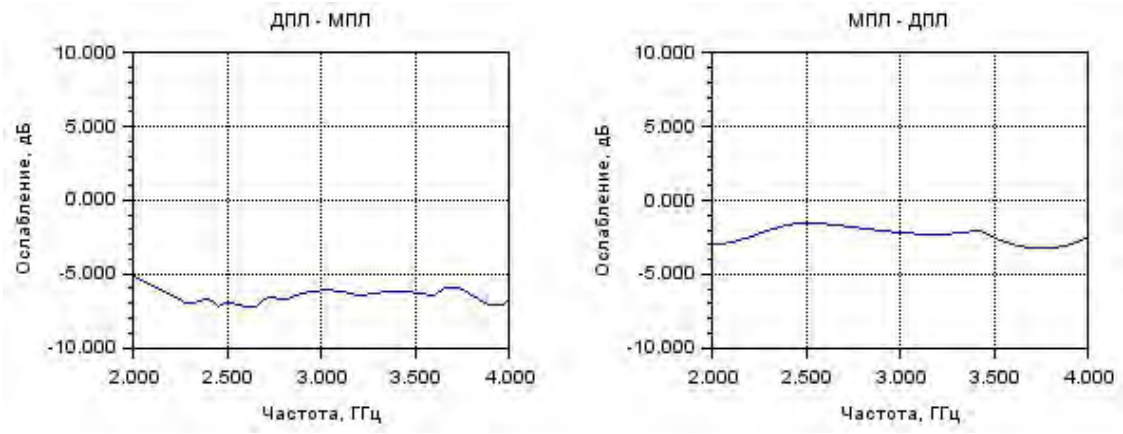


Рис. 5. Исследование полоскового перехода между МПЛ и ДПЛ

Заключительным этапом синтеза было создание Т - делителя СПЛ с переходом на две МПЛ (рис. 6) с учётом полученных ранее результатов.

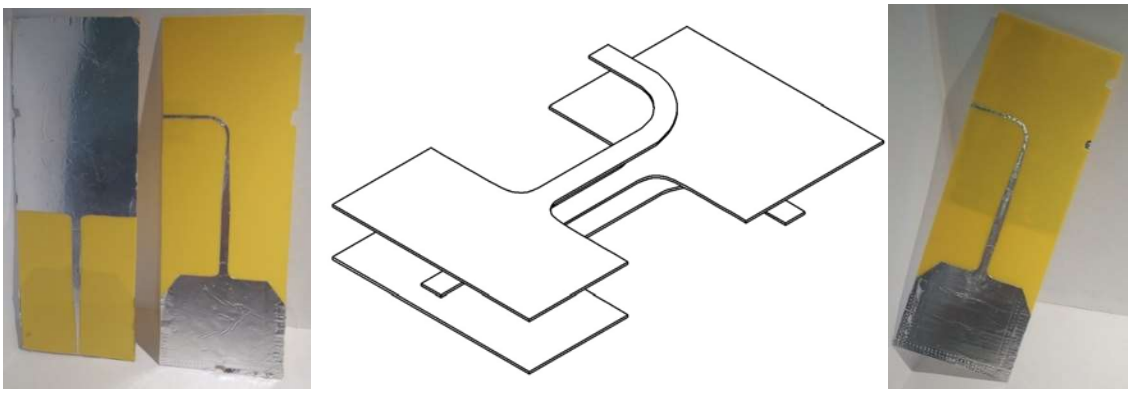


Рис. 6. Структура исследуемого делителя мощности

Были изготовлены различные масштабные макеты полоскового делителя мощности: макет с удлинённой согласующей ТПЛ, макет с укороченной согласующей ТПЛ. Результаты эксперимента представлены на рис. 7–8.

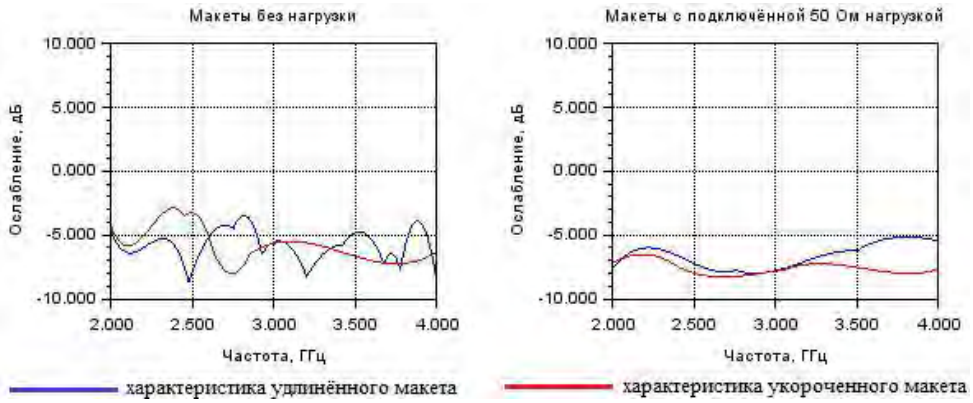


Рис. 7. Характеристики ослабления исследуемых макетов в диапазоне (2 – 4) ГГц

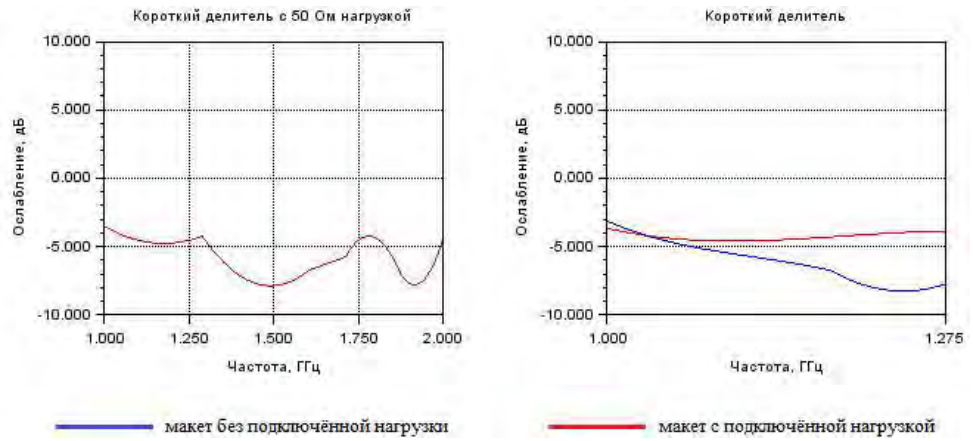


Рис. 8. Характеристика ослабления макета делителя с укороченной ТПЛ в диапазоне 1–2 ГГц

Исследуемые макеты делителя мощности обладают величиной ослабления на уровне –4 дБ в диапазоне частот 1–1,3 ГГц, что близко к ожидаемому значению –3 дБ.

Разработанный микроволновый сумматор с вводом/выводом энергии в разных слоях ОИС СВЧ является работоспособным в нижней части СВЧ диапазона. Используя принцип электродинамического подобия, рабочий диапазон сумматора можно повторять на различных участках СВЧ, изменяя масштаб конструкции. Использование промышленной технологии изготовления, однозначно, позволит добиться улучшения характеристик устройства.

Список используемых источников

1. Леонтьев А. С., Седышев Э. Ю. Синтез делителя мощности СВЧ в объёмном интегральном исполнении // Подготовка профессиональных кадров в магистратуре для цифровой экономики. Региональная научно-методическая конференция магистрантов и их руководителей (ПКМ-2020): сб. лучших докладов конф. / Сост. Н. Н. Иванов. СПб.: СПбГУТ, 2021 С. 335–338.

2. Ганстон М. А. Р. Справочник по волновым сопротивлениям фидерных линий СВЧ: пер. с англ. под ред. А. З. Фрадина. М.: Связь, 1976.

3. Вольман В. И. Справочник по расчету и конструированию СВЧ полосковых устройств. М.: Радио и связь, 1982.

4. Фельдштейн А. Л., Явич Л. Р., Смирнов В. П. Справочник по элементам волноводной техники. М.: Советское радио, 1967.

5. Боброва К. В., Булатова И. А., Иванова Е. А., Седышев Э. Ю. Расчёт модифицированных линий передач для объёмных интегральных схем // Электроника и микроэлектроника СВЧ. 2015. Т. 2. С. 161–170.

УДК 621.375
ГРНТИ 47.41.33

МОДЕЛИРОВАНИЕ И АНАЛИЗ ЧАСТОТНЫХ ХАРАКТЕРИСТИК КЛЮЧЕВЫХ ВЧ УСИЛИТЕЛЕЙ МОЩНОСТИ

М. А. Межевова, В. А. Филин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Описана методика компьютерного моделирования частотных характеристик ключевых (нелинейных) ВЧ усилителей мощности, работающих в режиме класса Е. Методика учитывает спектры реальных установившихся процессов, возникающих при наложении гармонического возмущения на периодическое управляющее воздействие. Приводятся и анализируются результаты расчетов.

высокочастотные ключевые усилители, метод эквивалентных частотных характеристик.

Классические усилители режимов А, АВ и В имеют значительно меньший средний КПД по сравнению с ключевыми усилителями. Одним из наиболее высокочастотных среди ключевых усилителей является режим класса Е [1], что является причиной повышенного интереса к нему исследователей и разработчиков ВЧ и СВЧ усилителей мощности. Минимизировать общие потери мощности, достичь высокого КПД позволяет поочередное формирование большого тока через транзистор при малом напряжении на нем и наоборот (рис. 1б).

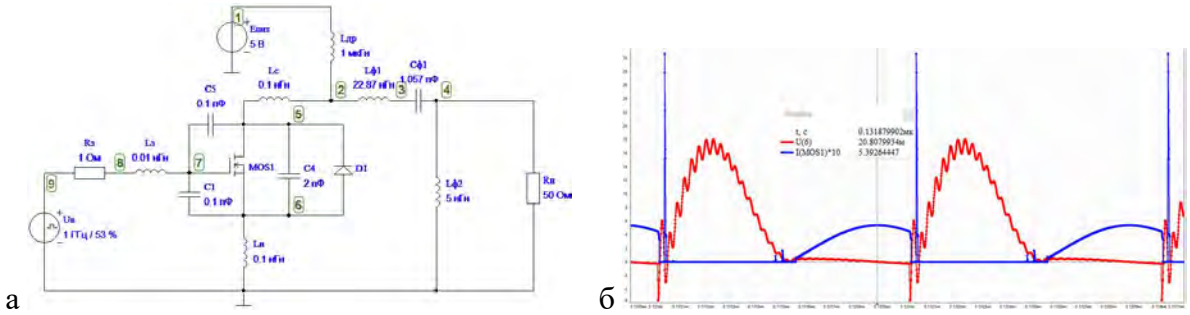


Рис. 1. Эквивалентная схема ключевого усилителя класса Е с учетом нелинейной динамической модели транзистора (а) и его переходная характеристика (б)

Особенностями модели усилителя мощности класса Е, используемой в данной работе и представленной на рис. 1а, является то, что транзистор описывается не в виде простого ключа, имеющего два состояния: включено (малое сопротивление) и выключено (большое сопротивление), а используется три состояния транзистора: отсечка, активный режим и насыщение [2, 3]. Данная модель транзистора позволяет более точно воспроизводить сложные процессы в ключевых генераторах, работающих на частотах сотен мегагерц - единиц гигагерц, в том числе исследовать влияние паразитных емкостей транзистора на устойчивость.

Энергетически эффективные ключевые усилители являются составной частью высокочастотной аппаратуры и должны удовлетворять жестким требованиям к стабильности своих выходных характеристик, обеспечивать высокую степень подавления собственных искажений и помех, обладать хорошими динамическими свойствами. Применение для задач анализа и синтеза ключевых устройств аппарата частотных характеристик может дать важную информацию для их рационального проектирования, обеспечения их устойчивости при работе со сложными нагрузками.

При анализе процессов в замкнутых нелинейных импульсных системах, к которым следует отнести ключевые ВЧ генераторы, принципиально важно учитывать реальные процессы, возникающие в кольце ООС. Однако, частотные методы анализа линейных схем не могут быть применены непосредственно для исследования цепей с нелинейными элементами.

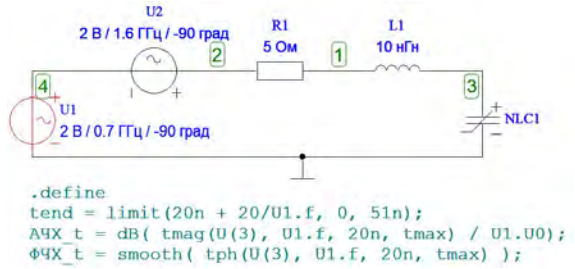
Рис. 2. Метод эквивалентных частотных характеристик

Рассмотрим метод эквивалентных частотных характеристик (рис. 2). На вход нормально функционирующей нелинейной системы подается гармоническое возмущение определенной амплитуды и частоты, после чего определяется реакция системы во временной области. Переходные процессы отбрасываются,

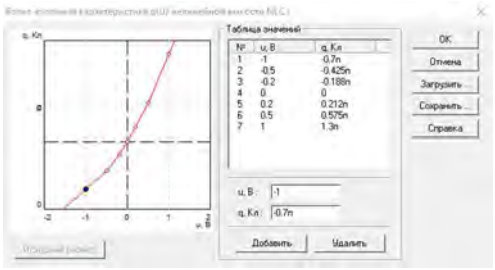
а из сложного установившегося процесса на основе гармонического анализа выделяются амплитуда и фаза составляющей, соответствующей по частоте гармоническому возмущению. По соотношениям амплитуд и фаз между реакцией и воздействием определяется одна точка ЧХ. При повторении этой процедуры на дискретных значениях частоты получается требуемая ЧХ исследуемой системы.

Этот алгоритм автоматизирован в программе FASTMEAN [4] и может быть применен для исследования различных классов нелинейных устройств, в частности ключевых ВЧ генераторов с внешним возбуждением (ВЧ усилителей мощности).

В качестве иллюстрации данной методики представлены результаты автоматизированного расчета АЧХ и ФЧХ коэффициента передачи колебательного контура, имеющего емкость с небольшой нелинейностью кулон-вольтной характеристики (рис. 3).



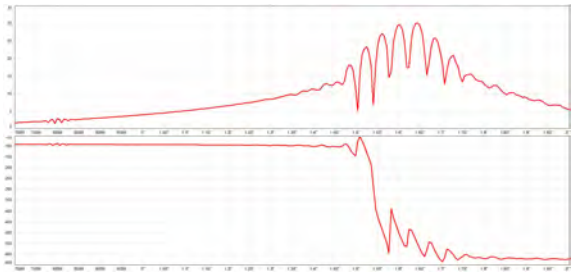
а



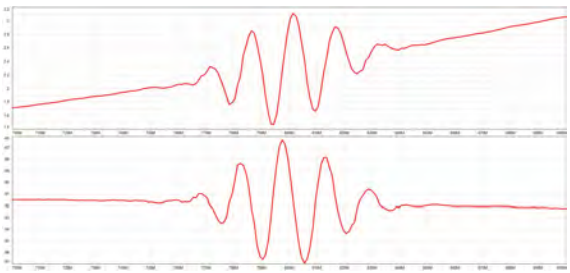
б

Рис. 3. Эквивалентная схема нелинейного колебательного контура (а); кулон-вольтная характеристика нелинейной емкости (б).

Из-за наличия нелинейности у емкости при определенных амплитудах воздействия в нелинейном контуре возникает дополнительный (нелинейный) резонанс на субгармонике (*fp*/2), который никак не предсказывается частотными методами анализа линейных схем.



а (0.7 ГГЦ-2 ГГц)



б (0.7ГГц-0.9ГГц)

Рис. 4. АЧХ и ФЧХ нелинейного колебательного контура (а); нелинейный резонанс на частоте *fp*/2 (б)

Этот резонанс приводит к реальному возникновению колебаний на частоте *fp*/2 (рис. 4), даже если этой частоты нет в спектре входного воздействия.

Применим рассматриваемый метод эквивалентных частотных характеристик к ВЧ генератору класса Е (рис. 5а). Данная схема имеет рабочую частоту близкую к резонансу на 1 ГГц. Моделирование и анализ установившегося режима показывает, что в схеме возникают колебания (рис. 5б,в) на субгармонике (частоте в два раза меньшей резонансной), вызванные влиянием нелинейных элементов.

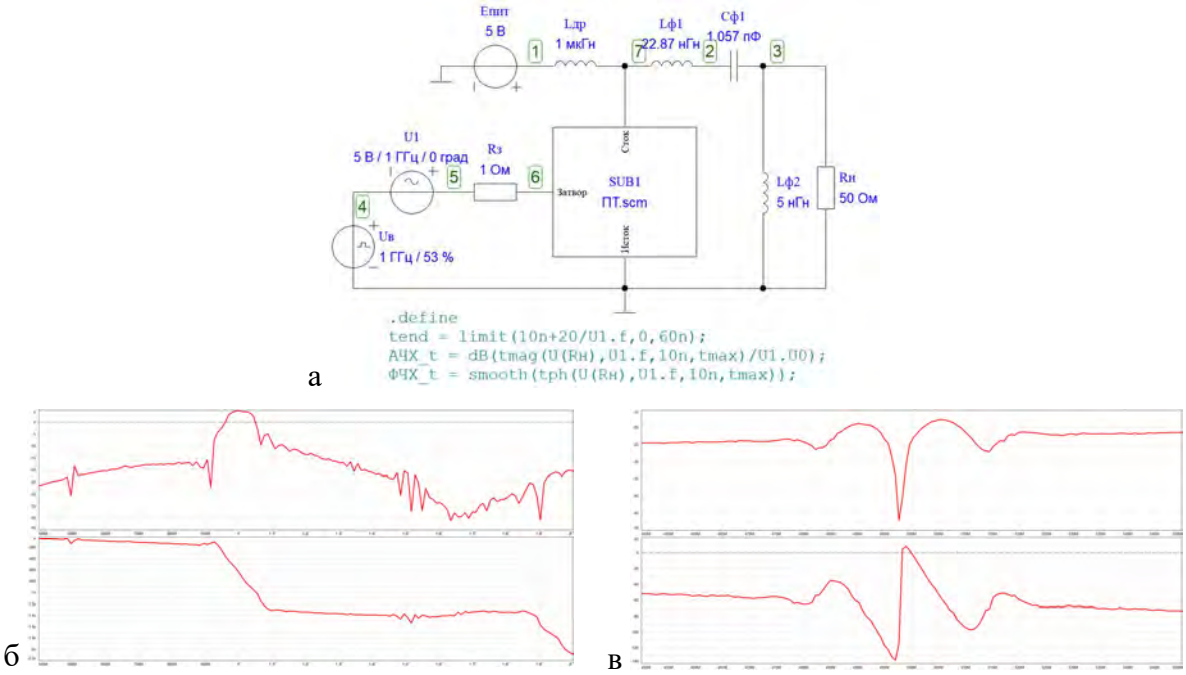


Рис. 5. Усилитель класса Е при введении гармонического возмущения (а) и его АЧХ и ФЧХ коэффициента передачи (б); (в) – АЧХ и ФЧХ вблизи субгармоники (*fp*/2)

Использование классических частотных методов для анализа существенно нелинейных схем, может привести к тому, что не будут выявлены реально возникающие автоколебания на субгармониках и дробных субгармониках (3/2 основной частоты). Эти автоколебания могут нарушить работу генератора, а в некоторых случаях привести к выходу транзистора из строя.

Метод эквивалентных частотных характеристик требует большого объема вычислений, поскольку он основывается на расчете *n* реализаций переходных и установившихся процессов в схеме для получения *n* точек частотных характеристик. На основе современных, эффективных в вычислительном отношении алгоритмов моделирования можно повысить скорость и точность численного расчета переходных и установившихся процессов в ключевых устройствах и тем самым обеспечить анализ их частотных свойств, в частности недостаточно изученный эффект дополнительных нелинейных резонансов на субгармониках тактовой частоты.

Список используемых источников

1. Grebennikov, Andrei; Sokal, Nathan O.; Franco, Marc J. Switchmode RF and Microwave Power Amplifiers // Academic Press, 2012. 704 p.
2. Ганбаев А. А. Формирование модулированных радиочастотных колебаний с улучшенными спектральными и энергетическими характеристиками в ключевых генераторах на GaN транзисторах: дис. … канд. техн. наук: 05.12.04 / Ганбаев Асиф Акиф оглы. СПбГУТ. СПб., 2020.
3. Ганбаев А. А., Филин В. А. Упрощенная динамическая модель мощных полевых транзисторов для исследования ключевых режимов радиочастотных устройств // Труды учебных заведений связи. 2019 Т. 5 № 2. С. 66–75. doi:10.31854/1813-324X-2019-5-2-66-75.
4. Смирнов В. С. Эквивалентные частотные характеристики транзисторных ключевых устройств с отрицательной обратной связью (математическое моделирование, методика измерения и оптимизации): дис. … канд. техн. наук: 05.12.04 / Смирнов Василий Сергеевич. СПбГУТ. СПб., 2006.

УДК 621.311.1(075)
ГРНТИ 47.49.02

ДИАГНОСТИКА ТЕХНИЧЕСКОГО СОСТОЯНИЯ ОБЬЕКТОВ ТЕПЛОЭНЕРГЕТИКИ НА ОСНОВЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Б. Ж. Мустагулова, А. Ж. Сагындикова

Алматинский университет энергетики и связи имени Гумарбека Даукеева

Представлено состояние теплоэнергетического оборудования Республики Казахстан. Показана необходимость создания современной системы, которая будет работать с использованием ретроспективных данных на основе распределенных вычислительных инфраструктур. Проанализированы современные информационные системы теплоэнергетической диагностики, предложены критерии контроля состояние теплоэнергетического оборудования по его состоянию, вопросы энергосбережения и эффективного использования энергоносителей являются основной проблемой национальной безопасности Республики Казахстан. Теплоэнергетический комплекс является основой энергетического сектора, анализ существующих информационных систем теплоэнергетического диагностирования и выработка критериев для дальнейшей разработки, внедрения и сопровождения ИС мониторинга и анализа режимов функционирования объектов теплоэнергетики с учетом их текущего технического состояния. В связи с этим актуальность создания информационной системы диагностирования и мониторинга состояния теплотехнического оборудования не вызывает сомнений.

теплоэнергетика, котельная, информационная система, диагностика, мониторинг, распределенная вычислительная инфраструктура.

Вопросы энергосбережения и эффективного использования энергоносителей являются основной проблемой национальной безопасности Республики Казахстан. Теплоэнергетический комплекс является основой энергетического сектора.

Основным источником получения тепла является котельная установка, это один из наиболее частых источников возникновения неисправностей, среди которых повреждение поверхностей нагрева котлов, систем топливоподачи, вспомогательного оборудования, автоматики и т. д. В таблице приведены распределение отказов оборудования энергоблоков мощностью 400 МВт [1, 2].

ТАБЛИЦА. Распределение отказов оборудования энергоблоков

Элементы	Процентное соотношение отказов, %
Поверхности нагрева	81,2
Дополнительное оборудование	4,5
Топливоподача, газопроводы	1,5
Регенеративные воздухонагреватели	0,3
Арматура	4,6
Автоматика и управление	7,4
Другое оборудование	0,5

На сегодняшний день 85 % теплоэнергетического оборудования в Республике Казахстан вырабатывает свой ресурс, в связи с этим возникает проблема создания систем контроля, технической диагностики и мониторинга теплоэнергетического оборудования. К основным причинам отказов котлов, вспомогательного оборудования котельных установок относятся неполадки и неисправности дымососов, дутьевых вентиляторов, регенеративных воздухоподогревателей и др.

Низкая надежность теплотехнического оборудования приводит к авариям и значительным потерям теплоты и, как следствие, к большим экономическим затратам и значительному количеству ремонтных работ. Статистика повреждения и теплопотерь в тепломагистралях РК на рис. 1 [3].

Рис. 1. Статистика повреждений и теплопотерь в тепломагистралях РК

Для повышения надежности теплоэнергетического оборудования необходимо накопление и систематизация данных длительной эксплуатации установок, которые производились раньше, и создание на этой основе установок, которые будут приспособлены к определенным условиям эксплуатации [4].

Целью работы является анализ существующих информационных систем (ИС) теплоэнергетического диагностирования и выработка критериев для дальнейшей разработки, внедрения и сопровождения ИС мониторинга и анализа режимов функционирования объектов теплоэнергетики с учетом их текущего технического состояния. Для диагностирования теплотехнического оборудования применяется разрушающий и неразрушающий контроль.

Разрушающий контроль (РК) – это совокупность методов измерения и контроля показателей качества изделия, по завершении которого нарушается пригодность объекта контроля к использованию по назначению. Позволяет контролировать качество материалов конструкций и их элементов, определять предел прочности и надежности. Преимущество разрушающего контроля состоит в том, что он позволяет получать количественные характеристики материалов.

Неразрушающий контроль (НК) – это контроль свойств и параметров объекта, при котором не должна быть нарушена пригодность объекта к использованию и эксплуатации. Метод является основным при проведении диагностики состояния оборудования и элементов конструкций, которые требуют особой надежности. Преимущество неразрушающего контроля состоит в том, что не требуется выведение объекта из рабочего режима либо его демонтаж.

Достоинства методов неразрушающего контроля (МНК): сравнительно большая скорость контроля, высокая надежность (достоверность) контроля, возможность механизации и автоматизации процессов контроля, возможность применения МНК в пооперационном контроле изделий сложной

формы, возможность применения МНК в условиях эксплуатации без разборки машин и сооружений и демонтажа их агрегатов, сравнительная дешевизна контроля и др. Одним из наиболее частых распространённых методов неразрушающего контроля для контроля теплотехнического оборудования является дефектоскопия. Дефектоскопия – это совокупность методов, которые выявляют дефекты конструкций, оборудования на предприятиях, металлических изделий и заготовок. Основной принцип проведения дефектоскопии (или метод неразрушающего контроля) – выявление потенциально опасных участков для предупреждения аварий, при этом не технологический процесс не должен быть остановлен, а демонтаж объекта исследования не требуется. Тщательный контроль – залог безопасности. Особо важные объекты, которые интенсивно эксплуатируются, проверяются регулярно.

В зависимости от физических явлений МНК подразделяют на 9 видов: акустический, ультразвуковой (магнитный), вихретоковый, проникающими веществами, радиоволновый, радиационный, оптический, тепловой, электрический. Под акустическим видом неразрушающего контроля понимают вид, основанный на регистрации параметров упругих колебаний, возбуждаемых и (или) возникающих в контролируемом объекте, рис. 2.

Рис. 2. Акустический вид неразрушающего контроля

В акустическом виде неразрушающего контроля чаще всего применяют звуковые и ультразвуковые частоты, т. е. используют диапазон частот приблизительно от 25,73 до 350 Гц. В случае, когда при контроле используют частоты свыше 20 Гц, допустимо применение термина «ультразвуковой» вместо термина «акустический», рис. 3. По характеру взаимодействия упругих колебаний с контролируемым материалом акустические методы подразделяют на следующие основные методы: прошедшего излучения (теневой, зеркально-теневой); отраженного излучения (эхо-импульсный); резонансный; импедансный; свободных колебаний; акустико-эмиссионный.

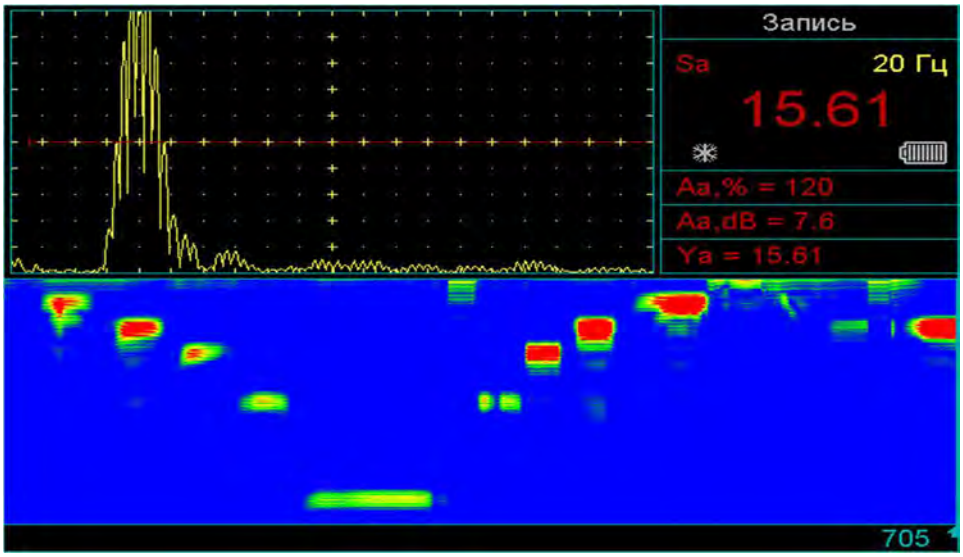


Рис. 3. Диагностика труб – дефекты коррозии внутренней поверхности трубы

Акустические методы по характеру регистрации первичного информативного параметра подразделяются на амплитудный, частотный, спектральный, решают следующие контрольно-измерительные задачи: метод отраженного излучения обнаруживает дефекты типа нарушения сплошности, определяет их координаты, размеры, ориентацию путём прозвучивания изделия и приёма отраженного от дефекта эхо-сигнала; резонансный метод применяется в основном для измерения толщины изделия (иногда применяют для обнаружения зоны коррозионного поражения, непропаев, расслоений в тонких местах из металлов); акустико-эмиссионный метод обнаруживает и регистрирует только развивающиеся трещины или способные к развитию под действием механической нагрузки.

Вихретоковый контроль трубопроводов выявляет микротрещины поверхности труб и сварных швов в местах изгибов и деформации трубы трубопровода. Вихретоковый контроль трубопроводов можно применять в условиях высоких температур стенок труб, где неприменим капиллярный контроль поверхности.

По результатам применения активного акустического МНК представленного на рис. 4, представлено, что в левой части рисунка изображен объект, не имеющий дефектов и соответствующий его проверке график, на котором отображены информативные параметры акустической волны (в данном случае время прохождения через объект). Справа изображен график, соответствующий наличию дефекта.

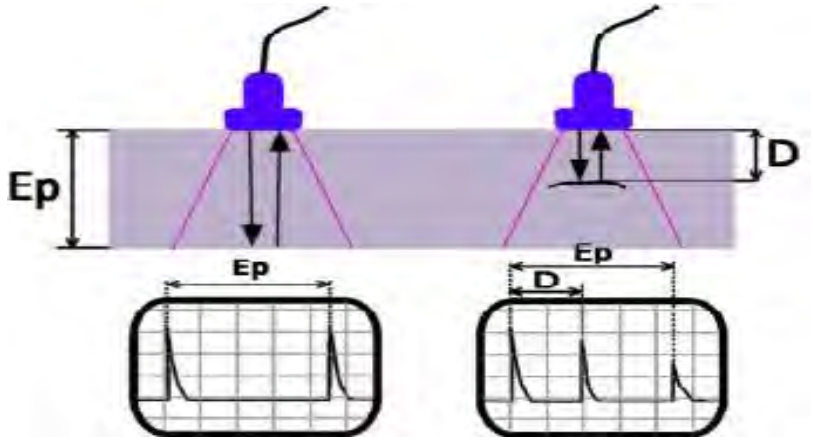


Рис. 4. Результат применения активного акустического МНК (отражения)

Современные технологии, в частности Internet of Things (IoT, «интернет вещей»), открывают новые возможности для улучшения существующих систем. Применение такой технологии приведет к увеличению эффективности, снижению издержек, внедрение энергосберегающих технологий. IoT – это глобальная сеть подключенных к Интернету физических устройств – «**вещей**», оснащенных сенсорами, датчиками и устройствами передачи информации. Эти устройства объединены посредством подключения к центрам контроля, управления и обработки информации.

На рис. 5 показана упрощенная структурная схема разрабатываемой ИС. С помощью сенсоров возможно будет получать данные и накапливать их в течение продолжительного времени. В случае возникновения внештатной ситуации, фиксируются ее параметры, а также принятые действия. Это позволит построить прогнозирующую модель, которая позволит по накопленным данным не только предвидеть те или иные события, но и выработать рекомендации для дальнейшего функционирования объекта диагностики.

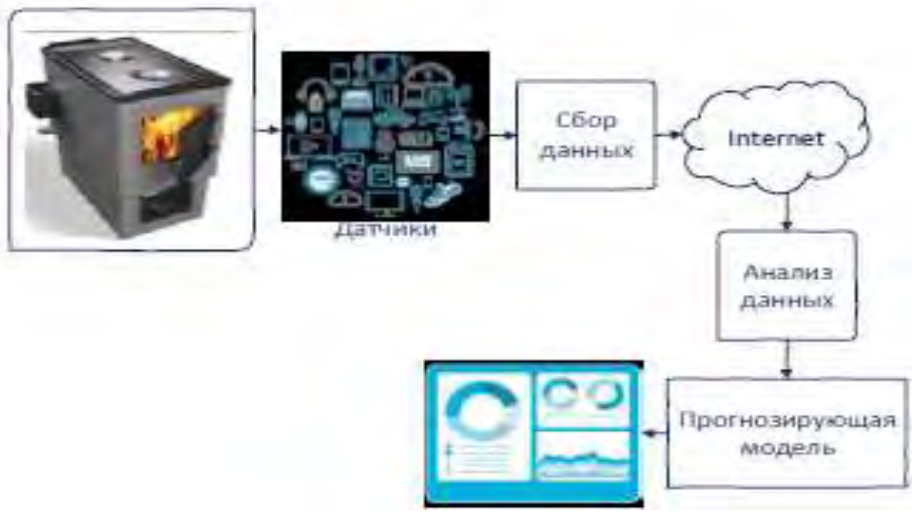


Рис. 5 Структурная схема разрабатываемой ИС

Базой для создания диагностических моделей могут служить процессы Бунимовича-Райса (модели шумовых сигналов) [5]. Простейшей диагностической моделью могут служить процессы Бунимовича-Райса:

$$\xi(t) \quad = \sum_{k=1}^{v(t)} \eta_к h(t-t_к),$$

где $v(t)$ – однородный процесс Пуассона с интенсивностью λ описывает число импульсов на интервале [0, t]; моменты времени возникновения импульсов $t_к$ являются однородным пуассоновским потоком событий; неслучайная функция $h(t)$ интенсивности появления импульсов λ. Поэтому диагностическими признаками могут являться вероятностные характеристики шумовых сигналов [6].

В заключение проведенного анализа установлено, что большая часть теплотехнического оборудования, которое используется в Республике Казахстан, технологически и морально устарело. В связи с этим актуальность создания информационной системы диагностирования и мониторинга состояния теплотехнического оборудования не вызывает сомнений. В данной статье предложено создание нового типа ИС для теплотехнической диагностики, которая базируется на анализе ретроспективной информации с использованием распределенных вычислительных инфраструктур («облаков»). Наиболее вероятностный вариант реализации такой системы возможен с использованием цифровой технологии IoT. В настоящее время ведется анализ параметров контроля, необходимых для создания ИС. Одним из наиболее важных параметров станет состав дымовых газов, который можно измерять при помощи системы контроля за процессом горения.

Список используемых источников

1. Казаков А. В. Надежность, диагностика элементов энергетического оборудования. Томск: Изд-во Томского политехн. ун-та, 2010. 224 с.

2. Гладышев Г. П. и др.Надежность теплоэнергетического оборудования ТЭС и АЭС : учеб. пособие для вузов / Под ред. А. И. Андрющенко. М.: Высш. шк., 1991. 302 с. ISBN 5-06-001752-4.

3. Ахметзянов А. М., Дубравский Н. Г., Тунаков А. П. Диагностика состояния ВРД по термогазодинамическим параметрам. М.: Машиностроение, 1983. 206 с.

4. Бюргер И. А. Техническая диагностика. М.: Машиностроение, 1978. 240 с.

5. Вапник В. Н., Червоненкис А. Я. Теория распознавания образов. М.: Наука, 1974. 416 с.

6. Елисеев Ю. С., Крымов В. В., Малиновский К. А., Попов В. Г. Технология эксплуатации, диагностики и ремонта газотурбинных двигателей : учеб. пособие. М.: Высш. шк., 2002. 355 с.

УДК 621.396.6
ГРНТИ 47.47

ОСНОВНЫЕ НОРМИРУЕМЫЕ ПАРАМЕТРЫ ГЕНЕРАТОРОВ, УПРАВЛЯЕМЫХ НАПРЯЖЕНИЕМ

Ю. А. Никитин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрены основные нормируемые параметры генераторов высокочастотных колебаний, применяемых в современных синтезаторах частоты. Эти параметры позволяют получить полное представление о качестве формируемых колебаний и влиянии на них дестабилизирующих воздействий.

синтез частот, кольцо импульсно-фазовой автоподстройки частоты (ИФАП), генераторы, управляемые напряжением, побочные спектральные составляющие (ПСС), детектор, логарифмический детектор, положительная обратная связь, отрицательная обратная связь.

При всем разнообразии задач, решаемых с помощью систем синтеза частот (ССЧ) и различных способов их решения, методы синтеза условно можно разделить на две большие группы – методы пассивного синтеза частот и методы активного синтеза частот (рис. 1).

Поскольку генератор, управляемый напряжением – ГУН (перестраиваемый генератор ПГ, генератор, управляемый током ГУТ) является важным элементом синтезатора частот, его качество характеризуют набором параметров. С помощью одних оценивают качество выходного колебания, других – показывают параметры ГУН как элемента конструкции – его напряжение питания и потребляемый ток, габариты и т. д., третьи показывают степень защищенности ГУН от внешних дестабилизирующих факторов [1, 2, 3, 4].

Основные нормируемые параметры любого ПГ (ГУН) следующие:

– мощность выходного сигнала ГУН (*Output Power*) $P_{\text{вых}}$. Зависит от частоты и определяется типом используемого ГУН и его элементной базой. Количественно определяется мощностью частоты основной гармоники выходного квазигармонического сигнала на стандартной нагрузке ГУН (50 Ом) в середине рабочего интервала управляющего напряжения $E_{\text{упр}}$ при номинальной температуре окружающей среды (+25 °С). Величина $P_{\text{вых}}$ измеряется в децибелах относительно мощности 1 мВт: $P_{\text{вых}}$ [дБ мВт или *dBm*];

– зависимость выходной мощности $P_{вых}$ от температуры (*Output Power Change with Temperature*). Это изменение мощности сигнала основной гармоники на выходе ГУН от температуры;

– отклонение от номинальной величины мощности на выходе ГУН (*Output Power Variation*) в диапазоне управляющих напряжений $P_{вых}(E_{упр})$. Часто указывают разность между максимальным и минимальным уровнем мощности на выходе ГУН в допустимом интервале изменения управляющего напряжения при номинальной нагрузке (выражается в дБ);

– смещение частоты ГУНа (*Pushing*) $S_o = \Delta f/\Delta E_{упр}$ [МГц/В] при изменении напряжения источника питания. Смещение определяется при изменении напряжения питания на ±(0,1…0,5) В от его номинального значения для различных фиксированных величин напряжений настройки и номинальных температуре и нагрузке;

– скорость перестройки частоты (время переходного процесса ГУН) (*Tuning Speed, Response Time*) – время, которое требуется для установления выходной частоты ГУН на 90 % от ее конечного значения после начала ступенчатого воздействия на управляющий вход частоты ГУН. На быстродействие ГУНа влияет полоса пропускания по каналу управления (управляющему входу) (*tuning bandwidth*).

Эта величина является мерой инерционности установки выходной частоты ГУН по отношению к быстрым изменениям управляющего напряжения $E_{упр}$. Она определяется как частота (в кГц) гармонического напряжения на входе управления ГУН, при которой девиация частоты выходного сигнала уменьшается в $\sqrt{2}$ раз по сравнению с девиацией при медленном (квазистатическом) изменении $E_{упр}$ в тех же пределах;

– температурный коэффициент изменения частоты ТКЧ = $\Delta f/\Delta T$ (*Frequency Drift With Temperature*), измеряемый в [МГц/°С] при номинальной температуре +25 °С. Иногда указывают уходы частоты от номинального значения для предельно допустимых значений температуры окружающей среды (например, –55 °С и +85 °С);

– затягивание частоты ГУН – изменение частоты при вариациях фазы коэффициента отражения от нагрузки (*frequency pulling*). Ее определяют, как разность между максимальным и минимальным значениями (*peak to peak*) частоты [МГц *p-p*] для всех значений фазы коэффициента отражения от 0 до 180° при фиксированном коэффициенте стоячей волны, равном 2;

Коэффициент стоячей волны (КСВ) или *standing wave ratio* (SWR) характеризует степень согласования источника сигнала с нагрузкой. На практике часть передаваемой энергии всегда отражается от нагрузки и возвращается в генератор. Отраженная энергия вызывает ухудшение работы генератора, в частности, ухудшение стабильности выходного колебания. КСВ рассчитывается следующим образом:

$$\text{КСВ} = (U_{\text{пад}} + U_{\text{отр}}) / (U_{\text{пад}} - U_{\text{отр}}),$$

где $U_{\text{пад}}$ и $U_{\text{отр}}$ – амплитуды падающей и отраженной электромагнитных волн. При идеальном согласовании КСВ = 1, значения до 1,5 считаются приемлемым.

– коэффициент гармоник выходного напряжения ГУН (*Harmonic Content*). Это уровень гармонических составляющих выходного колебания. Измеряется в дБ по отношению к несущей (дБн, *dBc*);

– спектральная плотность мощности (СПМ) фазового шума (*phase noise*) $S\varphi(F)$, где $F = |f_{\text{выхВЧ}} - f|$ – отстройка от несущей частоты (*carier offset*). Фазовый шум оценивают, как СПМ одной боковой полосы (*Single Side Band Phase Noise*) в полосе 1 Гц по отношению к мощности несущей частоты при определенной отстройке от нее (например, 10 кГц). Фазовый шум измеряется в дБн/Гц [*dBc*/*Hz*] (например, –105 дБн/Гц при отстройке 10 кГц). Величина $S\varphi(F)$ падает по мере увеличения расстройки F, достигая минимального уровня «белого фазового шума» при отстройках порядка полосы пропускания резонатора [1].

Аналогичный параметр для амплитудного шума, как правило, для ГУН не нормируется и не измеряется. Это связано с тем обстоятельством, что в активных цифровых синтезаторах частоты на основе умножающих колец импульсно-фазовой автоподстройки частоты (ИФАП) в трактах преобразования и приведения частоты ГУН $f_{\text{выхВЧ}}$ к частоте опорного колебания $F_{\text{опНЧ}}$ происходит многократное ограничение амплитуды колебаний с переводом амплитудной модуляции в фазовую (угловую).

Спектральную линию автогенератора условно можно разделить на пьедестал и крылья (рис. 1, см. ниже). Крылья спектральной линии будут спадать до тех пор, пока не достигнут уровня тепловых шумов. Можно записать, что минимальная мощность тепловых шумов (шумов Найквиста) на выходе усилителя или генератора при комнатной температуре:

$$P_{\text{ш макс}}\,[\text{дБм}] = -174 + 10\lg\Delta F + N_F,$$

где ΔF – ширина полосы частот в Гц;

N_F – коэффициент шума активного прибора.

На рис. 2 и в таблице (см. ниже) приведены его основные электрические параметры микросборки ГУН MVCO-2040-SF отечественной компании «Микран» (г. Томск) [5]. Заметим, что перестраиваемые СВЧ генераторы этой компании *pin*-совместимы с аналогичными генераторами остальных производителей [1, 3].

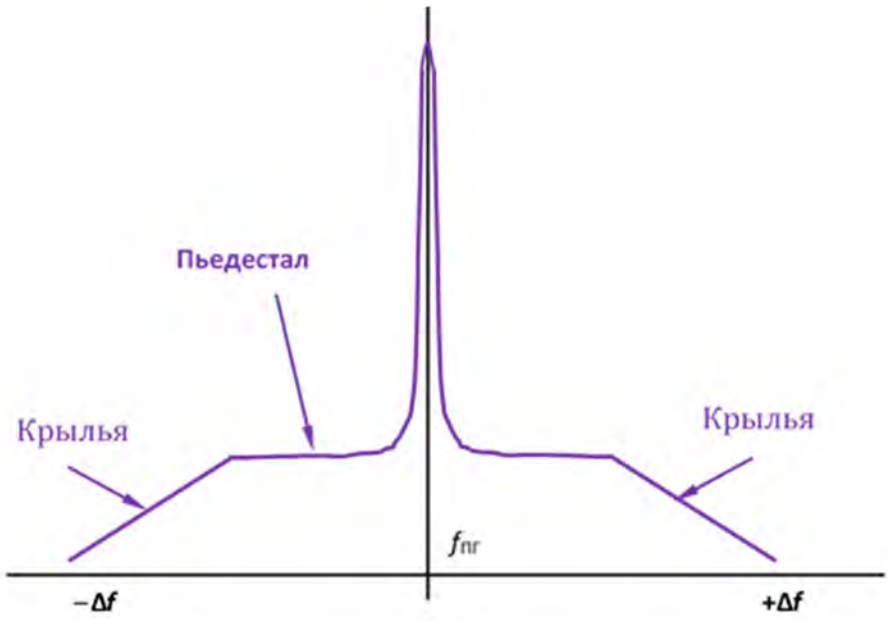


Рис. 1. Спектральная линия на выходе ПГ в петле ФАП

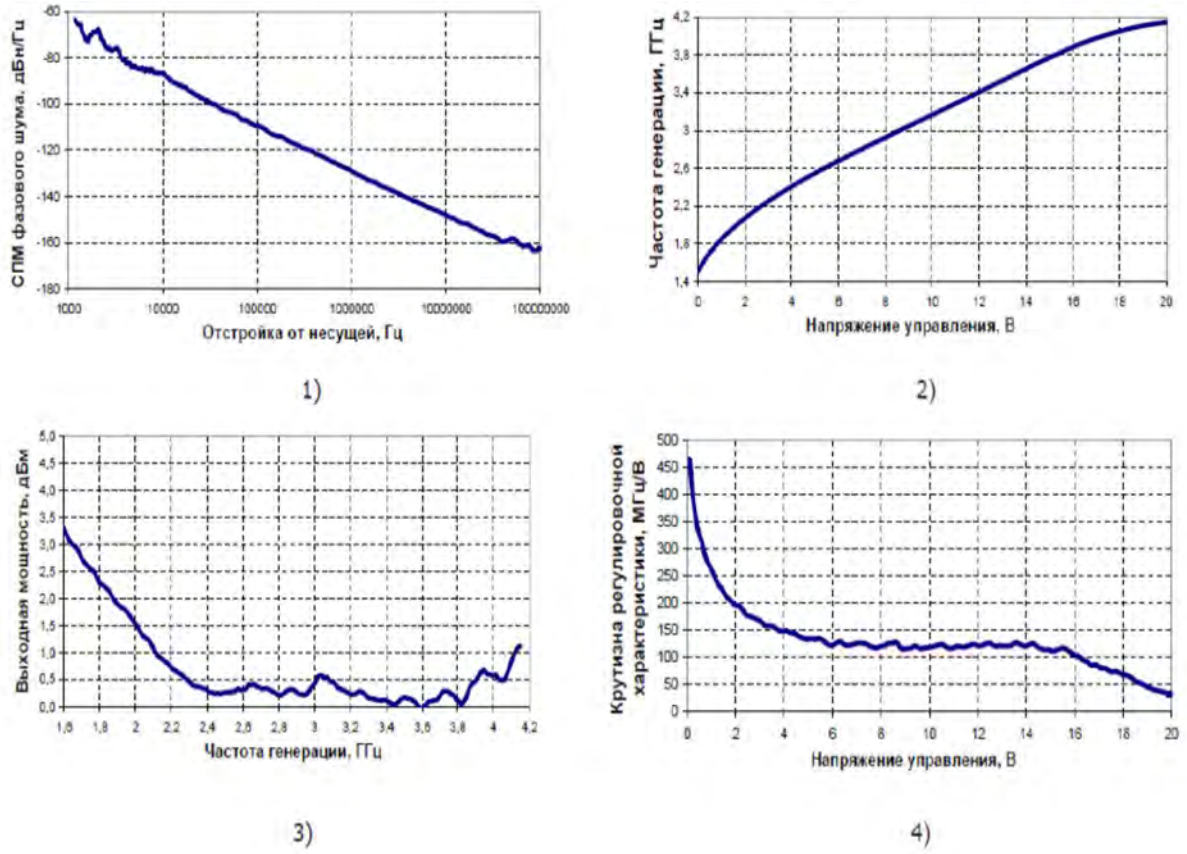


Рис. 2. Основные параметры выходного колебания СВЧ ГУН MVCO-2040-SF

Число нормируемых параметров генераторов постоянно растет, а их величины изменяются, что вызвано как многообразием принципов генерации и технических решений, так и многообразием задач, решаемых с помощью

генераторов в диапазоне частот от единиц герц до десятков терагерц вплоть до оптического диапазона [6].

ТАБЛИЦА. Электрические характеристики СВЧ ГУН MVCO-2040-SF

Параметр	Мин	Макс
Выходная частота, МГц	1600	4100
Фазовый шум на отстройке от несущей 100 кГц, в диапазоне 2–4 ГГц, дБн/Гц	–112	–106
Уровень второй гармоники, дБн	–15	
Напряжение управления, В	0	20
Крутизна регулировочной характеристики, МГц/В	50	450
Выходная мощность, дБм	0	5
Сопротивление нагрузки, Ом	50	
Емкость входа управления частотой, пФ	50	
Чувствительность к изменению напряжения питания, МГц/В	1,5	
Чувствительность к изменению нагрузки, МГц	–15	15
Рабочая температура, °С	–40	85
Изменение частоты, МГц в рабочем диапазоне температур	–20	20
Изменение выходной мощности в рабочем диапазоне температур, дБ	1,5	
Напряжение питания, В	5	
Ток потребления, мА	30	35

Список используемых источников

1. Voltage Controlled Oscillators (VCOs). URL: https://www.minicircuits.com/WebStore/Oscillators.html

2. Никитин Ю. А. Генераторы, управляемые напряжением производства Mini-Circuits для радиочастотных синтезаторов / Компоненты и технологии. 2003. № 3. С. 72–74.

3. Voltage Controlled Oscillator. URL: https://synergymwave.com/products/vco/

4. Никитин Ю. Генераторы, управляемые напряжением. Производства компании Synergy для радиочастотных синтезаторов / Электроника: наука. Технология, бизнес. 2005. № 5. С. 66–68.

5. СВЧ-Генераторы. URL: https://www.micran.ru/productions/IIS/svch/svch-generatory-/

6. Никитин Ю. А. Цифроаналоговый синтез частот. Теория и схемотехника : монография; СПбГУТ. СПб., 2018. 367с.

УДК 621.372.01
ГРНТИ 47.47

РАСЧЁТ УПРАВЛЯЕМОГО УСТРОЙСТВА ЗАДЕРЖКИ НАНОСЕКУНДНОГО ДИАПАЗОНА НА БИПОЛЯРНЫХ ТРАНЗИСТОРАХ ДЛЯ МОДИФИЦИРОВАННОГО КОНЕЧНОГО АВТОМАТА

Ю. А. Никитин, А. А. Синичкин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Произведен выбор и расчёт элементов для схемотехнического моделирования управляемого устройства задержки наносекундного диапазона. Проанализировано влияние паразитных емкостей элементов УУЗ на нелинейность преобразования цифрового кода управления во временной интервал. Схемотехническое моделирование выполнено в программном пакете Micro-cap. Для подачи сигнала переполнения на УУЗ используется модель конечного автомата построенного на основе делителя частоты с дробно-переменным коэффициентом деления и накапливающего сумматора.

управляемое устройство задержки, конечный автомат, накапливающий сумматор, делитель с дробно-переменным коэффициентом деления, Micro-cap.

Использование структуры двухуровневого МКА с управляемым устройством задержки (УУЗ) на идеальных элементах позволяет уменьшить ошибку воспроизведения колебаний синтезируемой частоты $f_{\text{выхНЧ}}$ на 105 дБ [1]. Последующая модель ГПН, реализованная с идеальным разрядным ключом напряжения позволила получить уровень дискретных побочных спектральных составляющих (ДПСС), кратных частоте шага сетки F_s на уровне 85 дБ [2].

Однако, при построении УУЗ на реальных элементах, выигрыш от ее введения в структуру конечного автомата (КА) будет ограничен рядом факторов, связанных с нелинейностью генератора пилообразного напряжения (ГПН), наличием паразитных ёмкостей активных приборов, конечным быстродействием компаратора и точностью (разрядностью) цифро-аналогово преобразователя [1].

Цель работы

Используя существующую электронную компонентную базу элементов спроектировать и рассчитать схему УУЗ наносекундного диапазона, имеющую низкий уровень ДПСС.

Основываясь на выбранной модели ГПН с ключом напряжения, хронирующей емкостью, идеальным генератором стабильного тока и диодом Шоттки в качестве ограничителя пилообразного напряжения (рис. 1), была спроектирована новая модель ГПН на основе реального генератора стабильного тока на биполярном транзисторе (рис. 2).

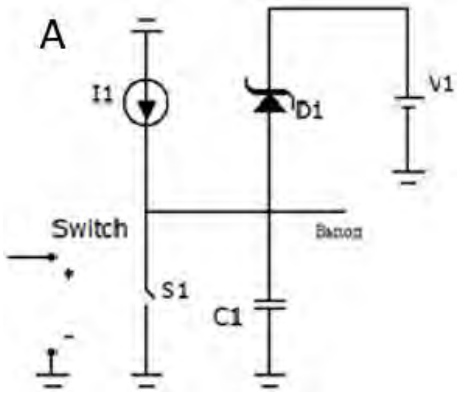


Рис. 1. Модель ГПН с идеальными ключом напряжения и генератором стабильного тока

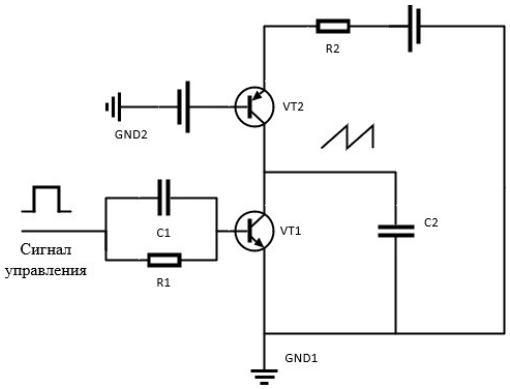


Рис. 2. Схема генератора пилообразного напряжения, построенного на генераторе стабильного тока, на биполярном транзисторе и ключе напряжения

Однако, значительное изменение паразитных ёмкостей в данной структуре оказывает сильное негативное влияние на линейность пилообразного напряжения (рис. 2). Расчеты и моделирование показали, что такая модель ГПН нуждается в дальнейшей модернизации.

Введение токовых ключей на дифференциальных каскадах позволяет уменьшить влияние паразитных ёмкостей транзисторов на конечный результат (рис. 3).

Дополнительно, для уменьшения влияния эффекта Миллера на линейность преобразования были выбраны транзисторы с минимальным значением ёмкости коллектор-база $C_{кб}$ и рассчитаны их параметры.

Расчёт $C_{кб}$ производился по формулам [3]:

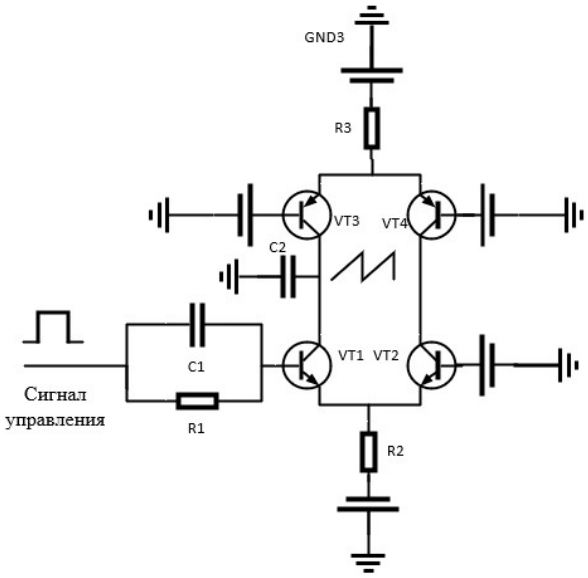


Рис. 3. Схема ГПН, построенного на токовых ключах

$$EG(T) = 1{,}16 - \frac{0{,}000702 * T^2}{T + 1108},$$

$$CJC(T) = CJT * (1 + MJC * (0{,}0004 * (T - T_{nom}) + \left(1 - \frac{VJC(T)}{VJC}\right),$$

$$VJC(T) = VJC * \frac{T}{T_{nom}} - 3 * VT * \ln\left(\frac{T}{T_{nom}}\right) - EG(T_{nom}) * \frac{T}{T_{nom}} + EG(T),$$

$$\mathrm{C_{кб}} = CJC(T)(1 - FC)^{-(1+MJC)} * (1 - FC(1 + MJC) + MJC * \frac{VBC}{VJC(T)}),$$

где *CJC* – емкость коллекторного перехода при нулевом смещении,

FC – коэффициент нелинейности барьерных емкостей прямосмещенных переходов,

MJC – коэффициент, учитывающий плавность коллекторного перехода,

T_{nom} – температура, при которой измерены модельные параметры,

T – рабочая температура,

VBC – напряжение между внутренними узлами базы и коллектора,

VJC – контактная разность потенциалов перехода база-коллектор.

Для моделирования временных и спектральных характеристик полученных электрических схем использовался SPICE-образный бесплатный программный пакет Micro-cap (рис. 4).

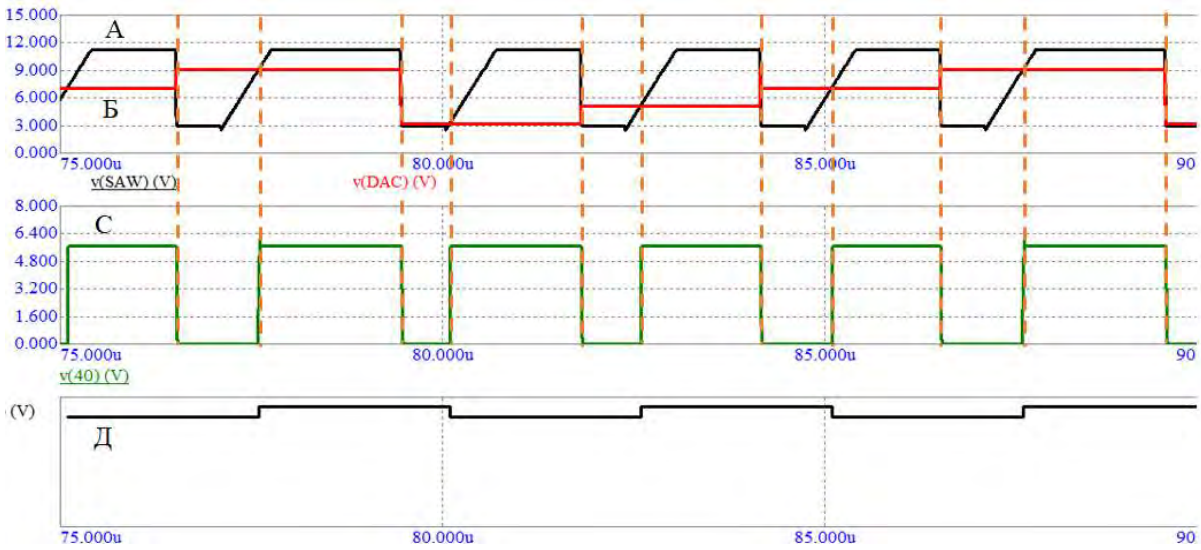


Рис. 4. Сигналы на входе компаратора: ГПН (А), выход ЦАП (Б).
Сигнал после компаратора (С), сигнал после *D*-триггера (Д).

По результатам моделирования реализация УУЗ на основе ГПН, построенного на токовых ключах на биполярных транзисторах, позволила уменьшить влияние паразитных ёмкостей транзисторов и повысить линейность преобразования цифрового кода управления во временной интервал.

Линеаризация пилообразного напряжения ГПН позволила уменьшить функциональную фазоимпульсную модуляцию синтезируемого колебаний на 74,5 дБ (рис. 5, 6).

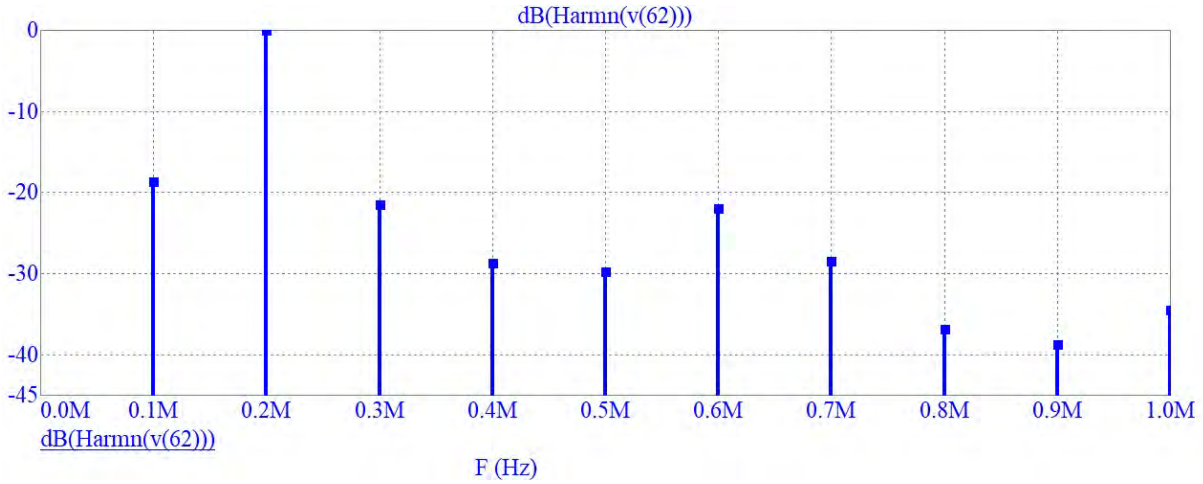


Рис. 5. Спектр выходного колебания КА без УУЗ
при частоте задающего генератора $f_{\text{опВч}} = 17$ МГц

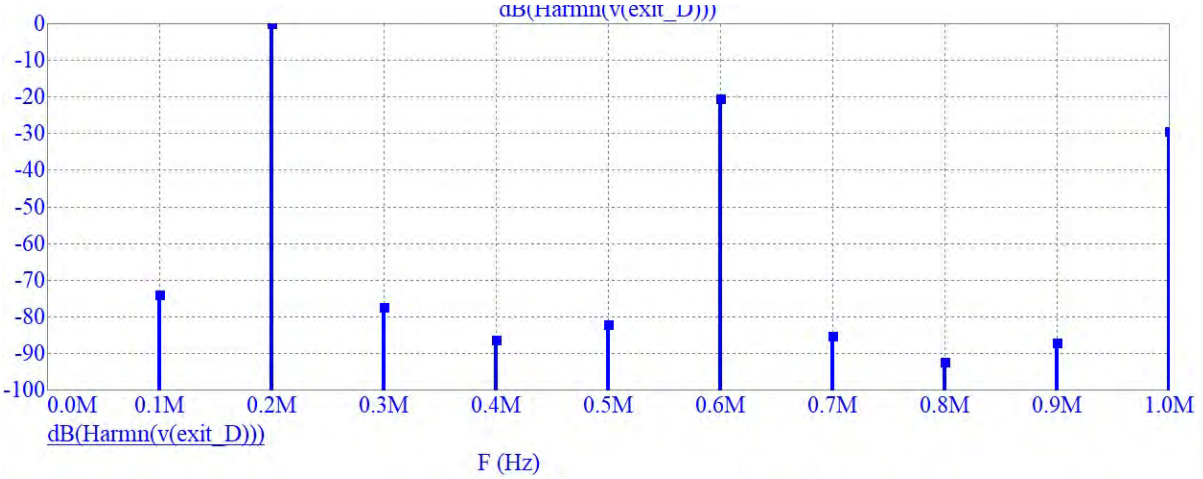


Рис. 6. Спектр выходного колебания КА с УУЗ
при частоте задающего генератора $f_{\text{опВч}} = 17$ МГц.

Список используемых источников

1. Никитин Ю. А. Цифроаналоговый синтез частот. Теория и схемотехника : монография; СПбГУТ. СПб., 2018. 367 с.

2. Никитин Ю. А., Синичкин А. А. Анализ структур конечных автоматов на основе накапливающего сумматора и делителя частоты с дробно-переменным коэффициентом деления для управляемого устройства задержки // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2020. Т. 3. С. 490–494.

3. Micro-Cap 10 Electronic Circuit Analysis Program Reference Manual 1982-2010 // Spectrum Software. South Wolfe Road Sunnyvale, CA 94086. Pp. 444–447.

УДК 621.391
ГРНТИ 47.01.05

МОДЕЛИРОВАНИЕ УМНОЖАЮЩЕГО КОЛЬЦА ИФАП С НЕЛИНЕЙНОСТЯМИ

Ю. А. Никитин, Г. А. Цыганков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается модель умножающего кольца импульсно-фазовой автоподстройки частоты в среде MicroCap12. При анализе используется нелинейная модель перестраиваемого генератора с характеристикой управления, задаваемой пользователем в виде функции, аппроксимирующей табличные значения. В модели применяется импульсно-фазовый детектор на основе двух частотно-фазовых детекторов со схемой подкачки заряда. Делитель с дробным переменным коэффициентом деления реализован по принципу дельта-сигма модулятора. Рассмотрена работа кольца в динамическом (при переключении коэффициента деления) режиме, а также спектр выходного колебания в установившемся (стационарном) режиме.

кольцо ИФАП, побочные спектральные составляющие, гетеродин, ИФД, ЧФД, автоподстройка частоты.

Для синтеза дискретно перестраиваемой, но стабильной частоты СВЧ диапазона применяются умножающие кольца импульсно-фазовой автоподстройки частоты (ИФАП) [1]. Для того, чтобы облегчить расчеты и исследовать фильтрующие, шумовые и временные характеристики кольца ИФАП удобно иметь его схемотехническую модель с управляющей характеристикой реального перестраиваемого генератора (ПГ).

Структурная схема моделируемого кольца ИФАП представлена на рис. 1. Были построены модели следующих структурных блоков: импульсно-фазовый детектор (ИФД), петлевой фильтр нижних частот, перестраиваемый генератор и делитель с дробно-переменным коэффициентом деления (ДДПКД). В качестве импульсно-фазового детектора для кольца ИФАП используется ЧФД на двух D-триггерах со схемой подкачки заряда.

Поскольку частота на выходе генератора определяется производной по времени от аргумента косинуса, а напряжение на входе является функцией от времени, в модели ПГ используется идеальный интегратор.

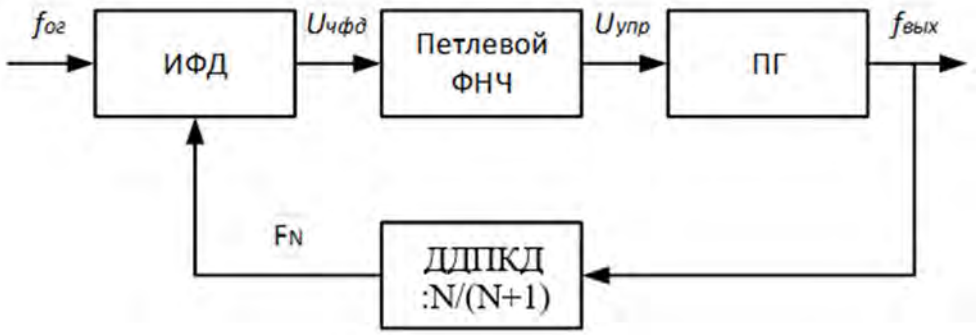


Рис. 1. Структурная схема кольца ИФАП

Макромодель нелинейного перестраимого генератора на основе источника тока, управляемого напряжением (ИТУН) показана на рис. 2.

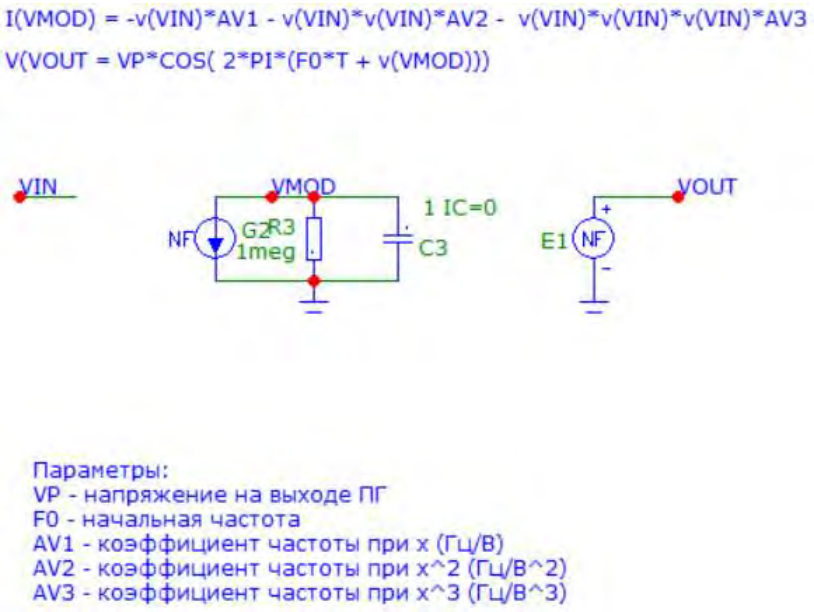


Рис. 2. Макромодель ПГ

Частота генерации определяется по формуле (1), где a, b, c и F_0 – коэффициенты, задаваемые пользователем.

$$f_{\text{выхВЧ}} = F_0 + a * U_{\text{вх}}^2 + b * U_{\text{вх}}^2 + c * U_{\text{вх}}^3, \quad (1)$$

Формулу можно изменять, меняя параметры ИТУН.

ДДПКД реализован с помощью дельта-сигма модулятора первого порядка на накапливающем сумматоре (НС). Делитель с целочисленным коэффициентом деления генерирует тактовые сигналы НС, к текущему значению которого каждый такт добавляется значение регистра a3 (дробная часть коэффициента). При переполнении НС, он формирует сигнал, который увеличивает целочисленный коэффициент деления на единицу

на одном периоде сравнения частот $T_{\text{опНЧ}}$. Таким образом, при 4-битном аккумуляторе достигается дробность коэффициента деления от 0 до 15/16.

В качестве фазового детектора использована схема ИФД на основе двух ЧФД. Данный фазовый детектор обеспеччивает крутизну статической характеристики $F'(\varphi_{\text{ст}}) = \frac{1}{2\pi}$. Данный детектор определяет и разность частот сигналов, что позволяет избежать ложных синхронизмов.

Петлевой фильтр нижних частот (ФНЧ) состоит из четырех RC звеньев, пропорционально-интегрирующего и изодромного звена и предназначен для фильтрации помехи с частотой сравнения в кольце ИФАП.

Для примера рассмотрим кольцо со следующими параметрами:

$$f_{\text{выхВЧ}}, \text{ГГц} = \left(0{,}8083 + 0{,}8695 * U_{\text{вх}} - 0{,}2325 * U_{\text{вх}}^2 + 0{,}02967 * U_{\text{вх}}^3\right);$$

$f_{\text{опНЧ}} \equiv F_{\text{ог}} = 10$ МГц – частота опорного генератора;

$U = [0..3{,}3]$В – управляющее напряжение на входе ГУН;

$N = 87\ldots229$ – диапазон коэффициентов деления;

$dN = \frac{1}{16}$ – шаг сетки коэффициентов деления;

$f_{\text{выхВЧ}} = [0{,}8725\ldots2{,}1825]$ГГц – диапазон синтезируемых частот;

$dF = 625$ КГц – шаг сетки;

$\tau = 0{,}17$ мкС – постоянная времени петлевого фильтра.

Сигнал с выхода петлевого ФНЧ после окончания переходного процесса представлен на рис. 6. Время переходного процесса определяется по уровню $U(F \pm 0{,}5\ dF)$.

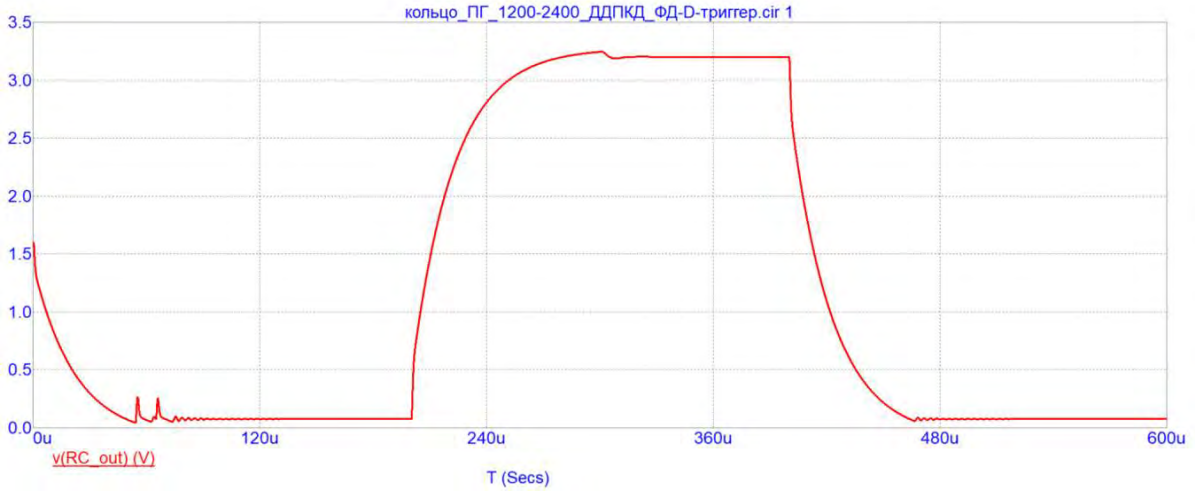


Рис. 3. Переходный процесс кольца ИФАП

Кольцо включается из исходного устойчивого состояния на свою минимальную частоту, при этом коэффициент деления:

N_{min} = (87 + 4/16), соответствующая частота $f_{выхВч}$ = 0,8725 ГГц. Длительность переходного процесса t = 114 мкС.

Затем, в точке 200 мкс, кольцо меняет коэффициент деления с минимального на максимальный:

N_{max} = (218 + 4/16), соответствующая частота $f_{выхВч}$ = 2,1825 ГГц. Длительность переходного процесса t = 85 мкС.

После чего, в точке 400 мкс кольцо вновь возвращается на минимальный коэффициент деления:

N_{min} = (87 + 4/16), соответствующая частота f = 0,8725 ГГц. Длительность переходного процесса t = 103 мкС.

Спектры выходной частоты генератора при разных коэффициентах деления N представлены на рис. 7 и 8.

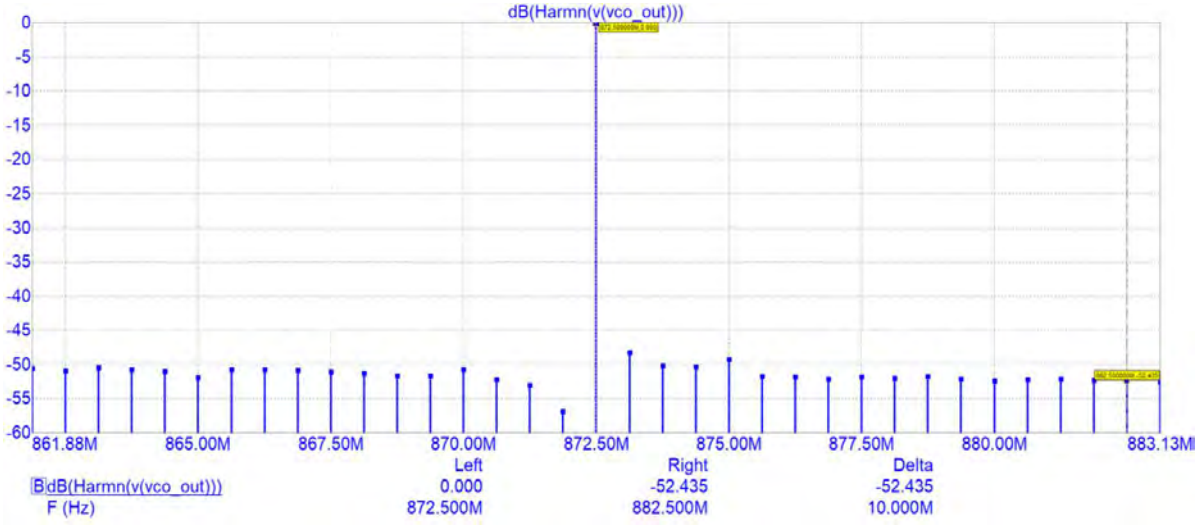


Рис. 7. Спектр выходного сигнала при N = 87 + 4/16

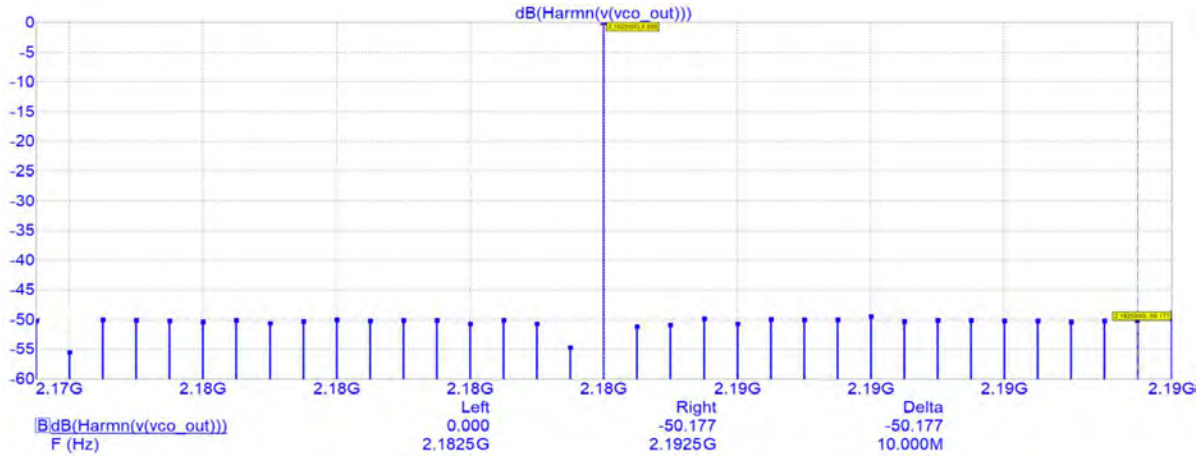


Рис. 8. Спектр выходного сигнала при N = 218+4/16

Как видно из графиков спектра, генерируемые частоты полностью совпадают с требуемыми. На спектрах частот выделены частоты сравнения, отстоящие от основной (синтезируемой) частоты на $f_{\text{опНЧ}} = 10$ МГц. Подавление частоты шага сетки и ее гармоник в модели составляет –47 дБ для $N_{\max}$ и –50 дБ для $N_{\min}$.

Разработанная схемотехническая нелинейная модель позволяет моделировать работу кольца ИФАП в статическом и динамическом режиме с учетом нелинейности перестраиваемого генератора и фазового детектора.

Список используемых источников

1. Никитин Ю. А. Цифроаналоговый синтез частот. Теория и схемотехника : монография; СПбГУТ. СПб., 2018. 367 с.

УДК 621.391
ГРНТИ 47.01.05

МОДЕЛИРОВАНИЕ ФАЗОВОГО ДЕТЕКТОРА НА ОСНОВЕ ДВУХ ЧФД

Ю. А. Никитин, Г. А. Цыганков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Исследуется модель фазового детектора, построенная в среде Microcap 12. Предложенная модель обладает единственным линейным участком передаточной характеристики (без периодичности), что позволяет перестраивать кольцо импульсно-фазовой автоподстройки по частоте, при этом сохранив малую величину зоны нелинейности, как у исходных частотно-фазовых детекторов со схемой подкачки заряда. Рассматриваются характеристики (статическая передаточная характеристика, величина зоны нелинейности) импульсно-фазового детектора в широком и узком диапазоне фазовых задержек. Произведен сравнительный анализ использования различных импульсно-фазовых детекторов (фазовый детектор на основе RS-триггера, частотно-фазовый детектор со схемой подкачки заряда) в кольце импульсно-фазовой автоподстройки частоты.

кольцо ИФАП, спектр частот, гетеродин, ИФД, автоподстройка частоты.

Одной из важнейших составных частей систем с импульсно фазовой автоподстройкой частоты (рис. 1) является импульсно фазовый детектор (ИФД). Принцип его работы заключается в формировании выходного напряжения, пропорционального разности фаз между опорным сигналом и сигналом перестраиваемого генератора, приведенным к частоте сравнения [1].

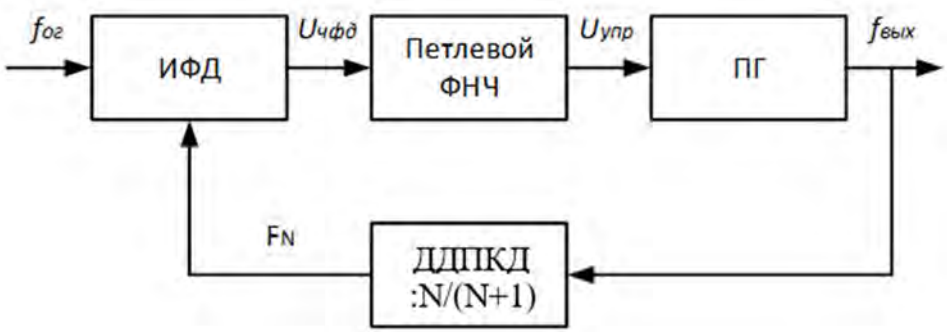


Рис. 1. Структурная схема кольца ИФАП

Простейшими фазовыми детекторами являются элементы «ИСКЛ. ИЛИ» и RS-триггер. Статическая характеристика схемы «ИСКЛ. ИЛИ» при подаче на ее входы меандров – «периодический треугольник»; статическая характеристика RS-триггера – «периодическая пила» представлена на рис. 2. Ее крутизна составляет $F'(\varphi_{ст}) = \frac{1}{\pi}$, характеристика периодична и повторяется каждые 2π периодов.

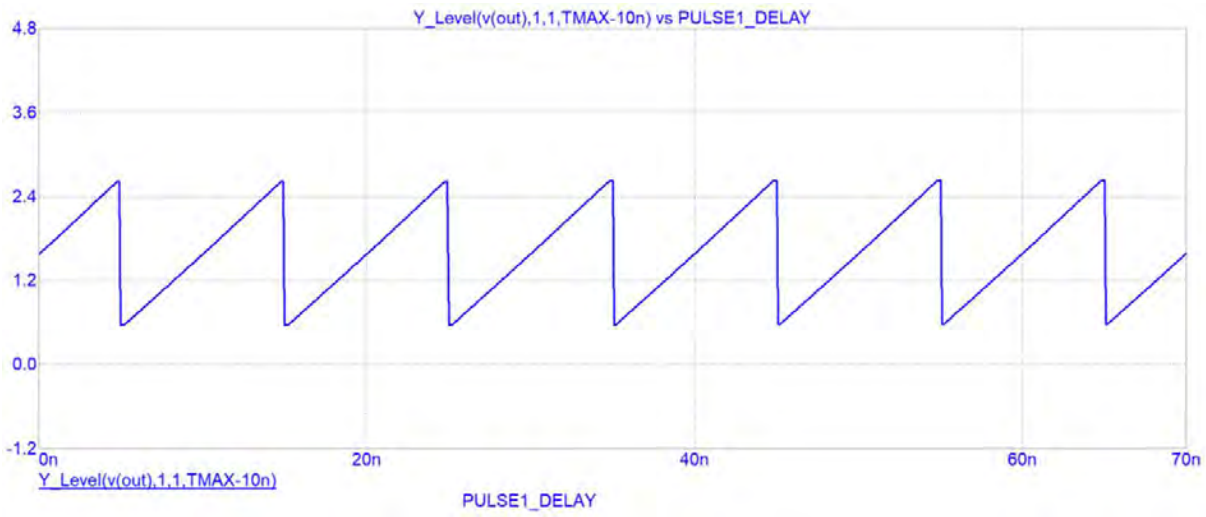


Рис. 2. Статическая характеристика RS-триггера

Периодичность статической характеристики ведет к ложным синхронизмам, поэтому зачастую применяются схемы на основе двух RS или D триггеров (ЧФД). В них за счет сшивки характеристик двух триггеров обеспечивается вдвое меньшая крутизна статической характеристики: $F'(\varphi_{ст}) = \frac{1}{2\pi}$. Статическая характеристика ЧФД представлена на рис. 3.

При равных частотах входных колебаний управляющая характеристика ЧФД практически линейна, однако из-за ее периодичности через каждые 2π возможно появление ложных синхронизмов при расстройке частот на входах ЧФД.

Рис. 3. Статическая характеристика ЧФД

Возникает потребность в новом типе фазового детектора, который бы отслеживал разность фаз сигналов, превышающею период, и, как следствие, мог бы различать сигналы по частоте.

Такой фазовый детектор можно реализовать, добавив к схеме ЧФД дополнительные триггеры, которые можно рассматривать как дополнительные ЧФД. Данные триггеры отслеживают, приходит ли во время периода сигнала со входа «1» два сигнала со входа «2», фиксируя, сигналы какого входа обладают большей частотой. И наоборот, триггеры отслеживают, приходит ли во время периода сигнала со входа «2» два сигнала со входа «1», фиксируя, сигналы какого входа обладают большей частотой.

Также добавлен компаратор, который на основе кода триггеров выставлял бы выходной сигнал в «+1» или «-1» на протяжении всего периода тактового сигнала. Схема, смоделированная в программе «Microcap» представлена на рис. 4.

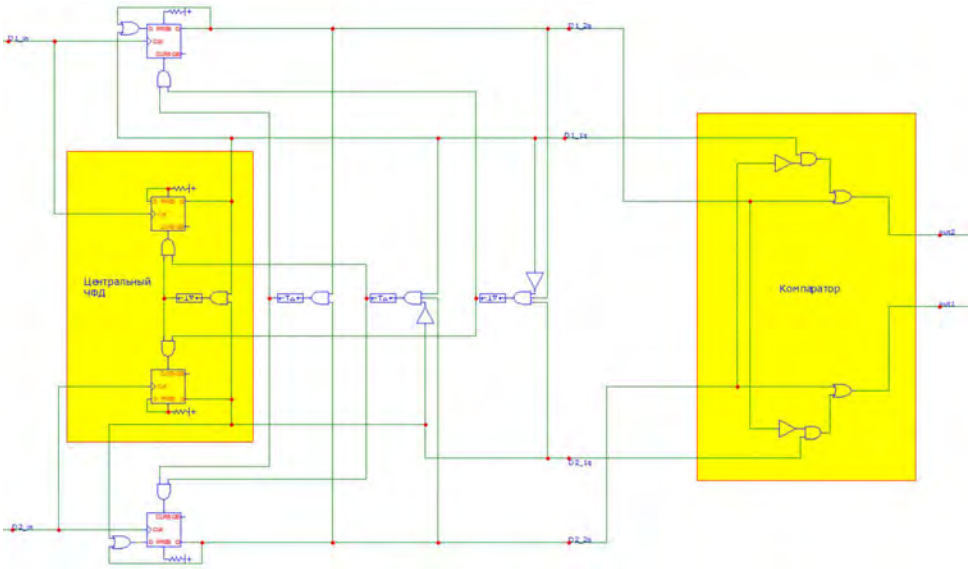


Рис. 4. Схема фазового детектора на основе двух ЧФД

Статическая характеристика представлена на рис. 5.

Зона нелинейности в окрестностях нулевого фазового сдвига для ИФД на основе двух ЧФД, как и в обычном ЧФД, определяется длительностью перепадов управляющих импульсов. При этом ее можно уменьшить вплоть до нуля при помощи устройства задержки сброса триггеров.

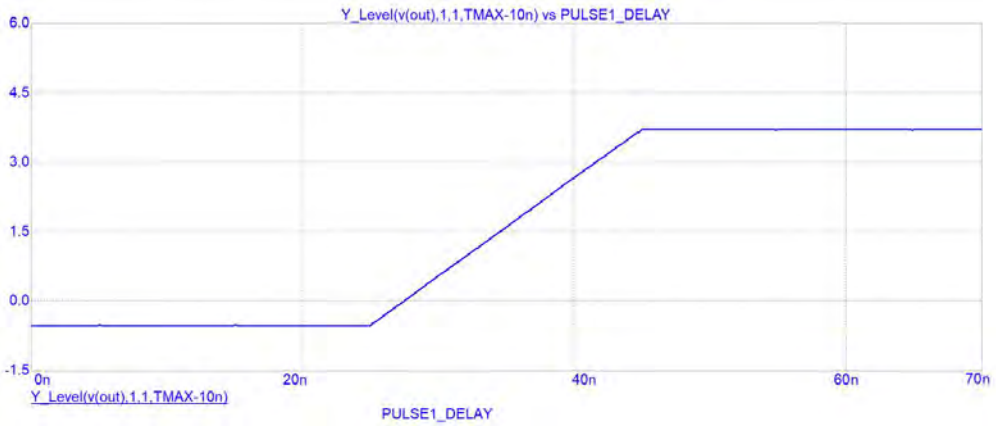


Рис. 5. Статическая характеристика ИФД на основе двух ЧФД

Вид зоны нелинейности при разных задержках сброса триггеров представлен на рис. 6 и 7.

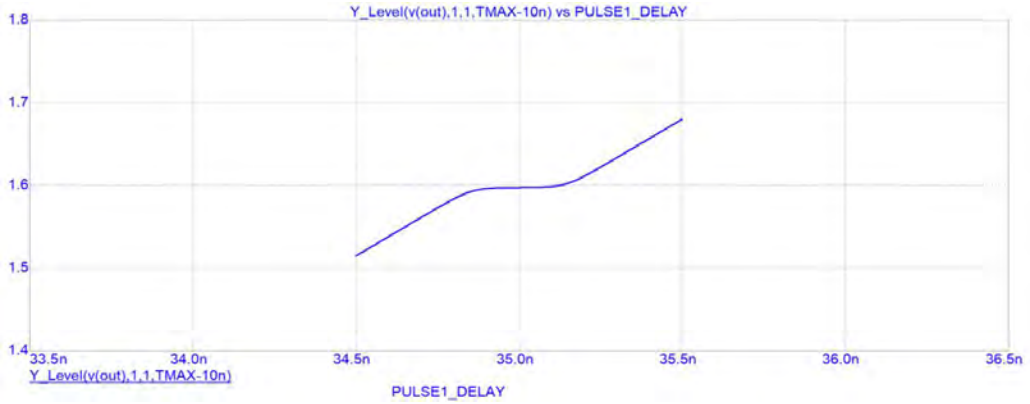


Рис. 6. Зона нелинейности при задержке сброса триггеров 0,01 нс

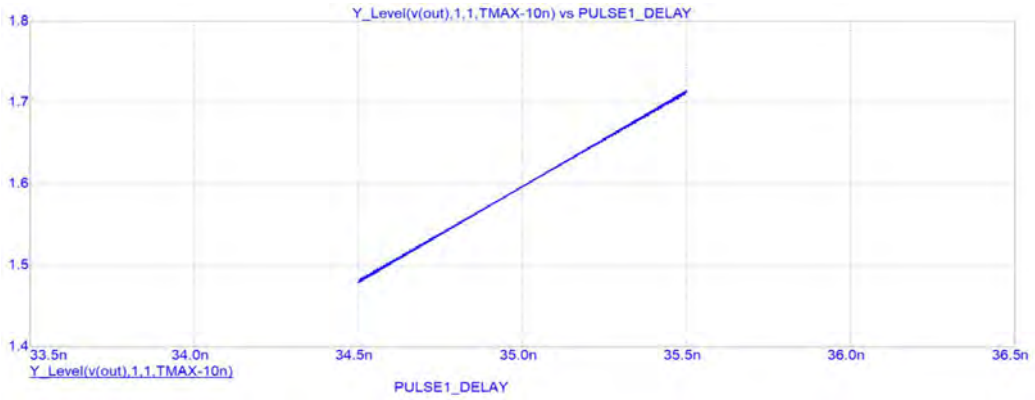


Рис. 7. Отсутствие зоны нелинейности при задержке сброса триггеров 1 нс

Благодаря исключению повторяемости статической характеристики исключаются ложные синхронизмы кольца ИФАП. Переходный процесс синхронизации кольца ИФАП с ЧФД представлен на рис. 8. Переходный процесс синхронизации кольца ИФАП с фазовым детектором на основе двух ЧФД представлен на рис. 9. Как видно, при использовании обычного ЧФД кольцо входит в ложные синхронизмы; при использовании фазового детектора на основе двух ЧФД этого не наблюдается.

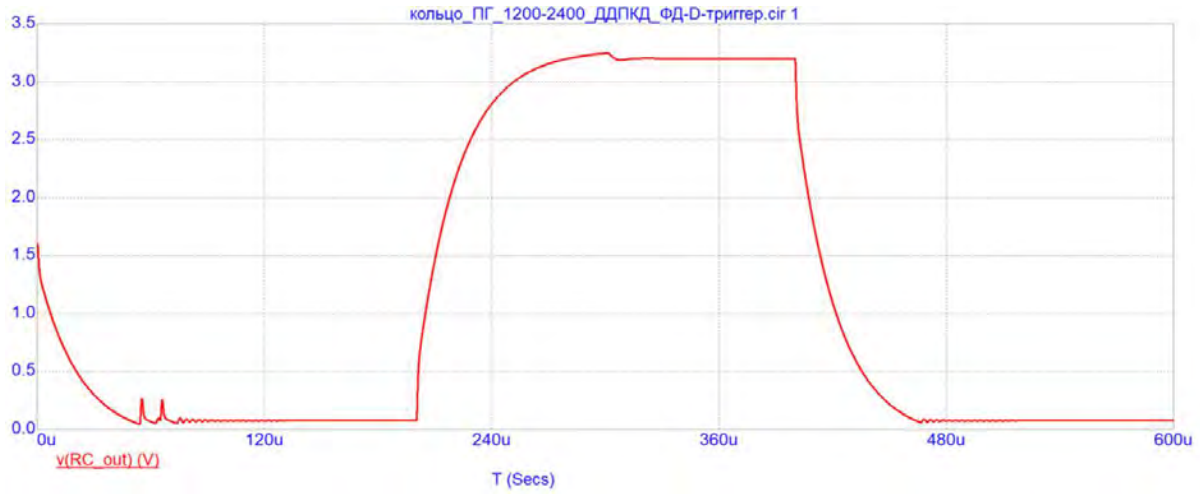


Рис. 8. Переходный процесс в кольце с ЧФД

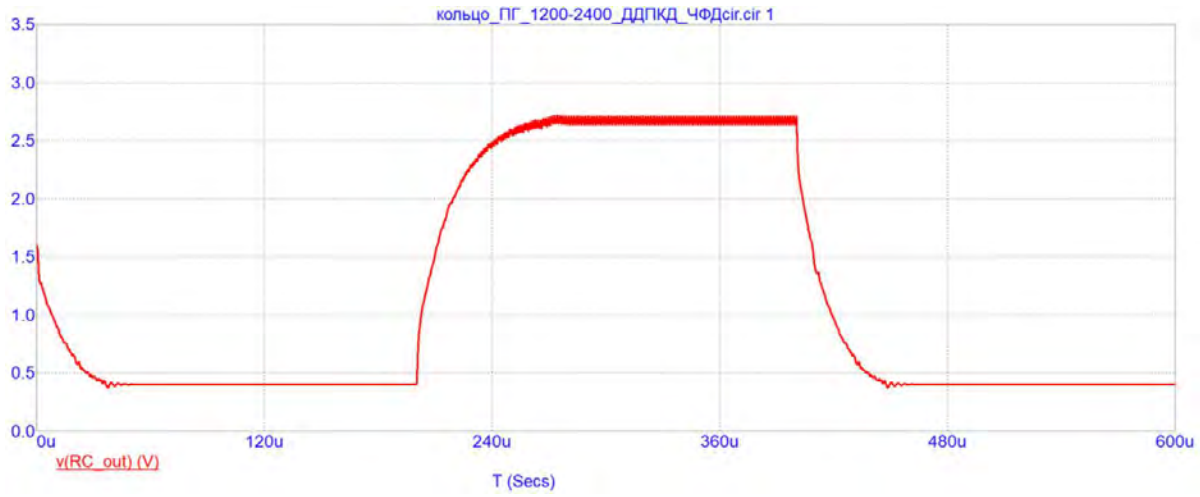


Рис. 9. Переходный процесс в кольце с ФД на основе двух ЧФД

Разработанная схема обладает основным преимуществом ЧФД – линейной крутизной управляющей характеристики, при этом в ней устранен один из существенных недостатков – повторяемость биений статической характеристики.

Список используемых источников

1. Никитин Ю. А. Цифроаналоговый синтез частот. Теория и схемотехника : монография; СПбГУТ. СПб., 2018. 367 с

УДК 621.3.029.63
ГРНТИ 47.45.99

МАСШТАБИРОВАНИЕ ТОПОЛОГИИ КАК МЕТОД СИНТЕЗА ПОЛОСКОВЫХ ФИЛЬТРОВ СВЧ

А. В. Полякова, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе рассматривается инженерный синтез СВЧ фильтров. Путём масштабирования геометрии полосно-пропускающего полоскового фильтра на связанных резонаторах, который выбирается в качестве прототипа, создаются масштабные макеты устройства с новыми техническими характеристиками.

Создаваемые фильтры исследованы на предмет смещения центральной частоты и изменения ширины полосы пропускания. Проведён анализ различных конструктивов полосовых фильтров и выбраны наиболее подходящие конструкции фильтров для применения методики масштабирования.

синтез, макетирование, полосно-пропускающий фильтр СВЧ, полосковый фильтр, шлейфный фильтр, фильтр с U-образными резонаторами, центральная частота.

Классический метод синтеза ППФ состоит в использовании фильтра-прототипа нижних частот и последующего частотного преобразования [1]. Создание простого инженерного метода синтеза ППФ СВЧ – актуальная задача СВЧ электроники. Такой метод упростит процесс разработки устройств частотной селекции, поможет избежать громоздких расчётов и сократит время синтеза фильтров.

Большинство работ по синтезу фильтров содержит таблицы и формулы пересчета параметров принципиальной схемы и конструкции, что говорит об отсутствии простых и эффективных способах расчета фильтров. Изготовление макетов методом масштабирования очень экономично и не требует временных затрат.

В качестве исходной конструкции для исследования взят полосовой полосковый фильтр на связанных резонаторах, представленный на рис. 1. Центральная частота этого фильтра, согласно проведённым измерениям, находится в районе 2,5 ГГц, результат представлен на рис. 2.

В начале работы был создан макет данного фильтра в масштабе 1:1, его вид представлен на рис. 3 (см. ниже). Геометрические размеры и топология слоя совпадают с геометрическими размерами исходного фильтра-прототипа, отличается лишь толщина подложки устройства.

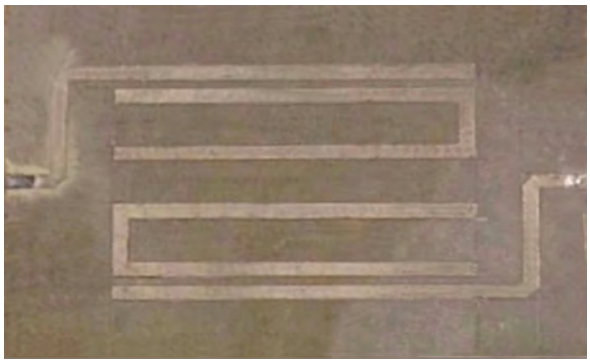


Рис. 1. Макет полосового полоскового фильтра

Рис. 2. Частотная характеристика макета

В результате оценочных измерений видим, что центральная частота созданного макета составляет 1,9 ГГц, что не совпадает с центральной частотой исходного фильтра. Это объясняется тем, что сохранена только топология, но не свойства диэлектрика. Затем макет подстраивался путем изменения *толщины* диэлектрического слоя, которая фактически изменила номинал волновых сопротивлений всех линий устройства.

В результате измерения, представленные на рис. 4, показали, что центральная частота сместилась в район 2,6 ГГц, что практически совпадает с центральной частотой фильтра-прототипа.

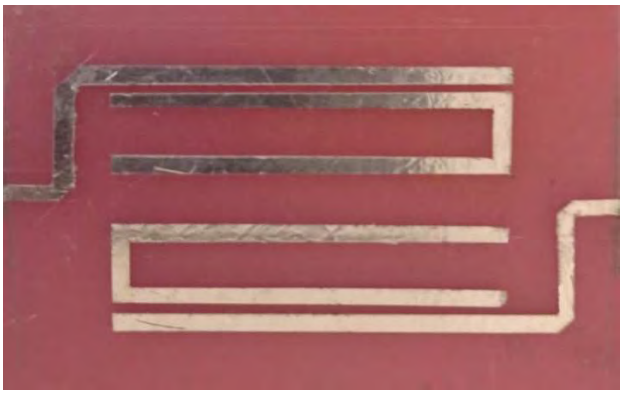


Рис. 3. Макет фильтра 1:1

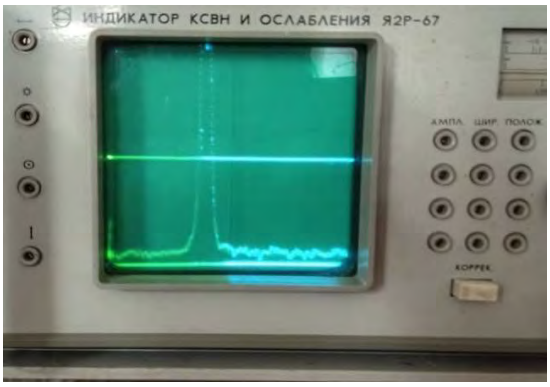


Рис. 4. Частотная характеристика макета 1:1

Таким образом, путём масштабирования топологии мы добились изменения частотных свойств фильтра, сохранив сам фильтр. С изменением геометрических размеров топологии фильтра-прототипа изменилась как центральная частота, так и ширина полосы пропускания фильтра.

Второй макет был создан с коэффициентом подобия 1,5, он изображен на рис. 5. Все геометрические размеры проводящего слоя топологии были увеличены в 1,5 раза. Измерения, представленные на рис. 6, показывают, что значение центральной частоты также увеличилось и составило 3 ГГц, однако из эксперимента видно, что мы имеем дело со 2 «паразитной» полосой пропускания. Но однозначно можно сказать, что центральная частота «ушла» с 2,5 ГГц.

Рис. 5. Макет фильтра 1:1,5

Рис. 6. Частотная характеристика макета

Масштабированием топологии добились изменения частотных свойств фильтра, сохранив сам фильтр. С изменением геометрических размеров топологии фильтра-прототипа изменилась как центральная частота, так и ширина полосы пропускания фильтра.

Из анализа полученных характеристик фильтра можно сделать вывод, что они зависят от ёмкостей между резонаторами. Если линейные размеры резонаторов должны изменяться прямо пропорционально частоте, то емкости связи очевидно должны изменяться по более сложному закону.

В связи с этим можно предположить, что существуют более простые топологии фильтров СВЧ, которые можно рассмотреть в начале нашей работы. Рассмотрим различные типы полосовых фильтров для дальнейшего исследования, а именно: шлейфный, ступенчатый, гребенчатый фильтры, фильтр на встречно-штыревой структуре и фильтр с краевой связью. Все эти структуры, которых приведены на рис. 7. В силу относительной простоты структуры выберем шлейфный полосовой фильтр.

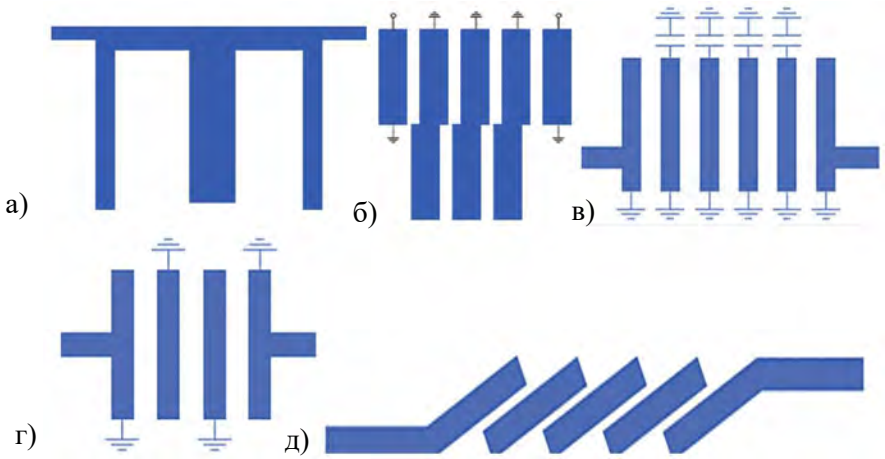


Рис. 7. Структуры различных типов полосковых фильтров СВЧ: шлейфный (а), ступенчатый (б), гребенчатый (в), на встречно-штыревой структуре (г), со связью по краям (д)

Синтез шлейфного полосового фильтра с параллельными четвертьволновыми шлейфами и четвертьволновыми соединительными линиями заключается в синтезе фильтра-прототипа нижних частот, его расчёте, частотном преобразовании и расчёте геометрических параметров шлейфного полосового фильтра [2, 3]. Для рассмотрения был взят уже рассчитанный шлейфный фильтр, представленный на рис. 8.

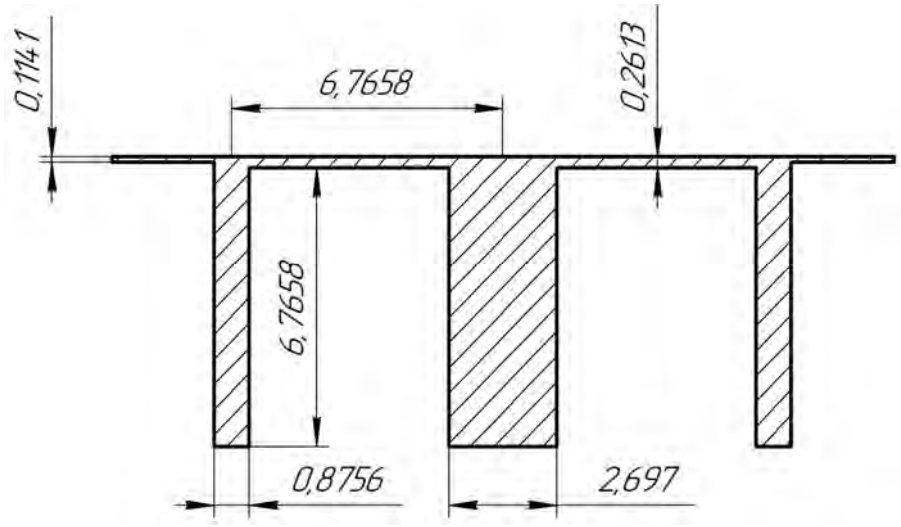


Рис. 8. Эпюр шлейфного полосового фильтра с параллельными четвертьволновыми шлейфами и четвертьволновыми соединительными линиями

При эмуляции данного фильтра в САПР RFSim99 была получена его АЧХ, рис. 9, из которой видно, что центральная частота составляет 3,2 ГГц.

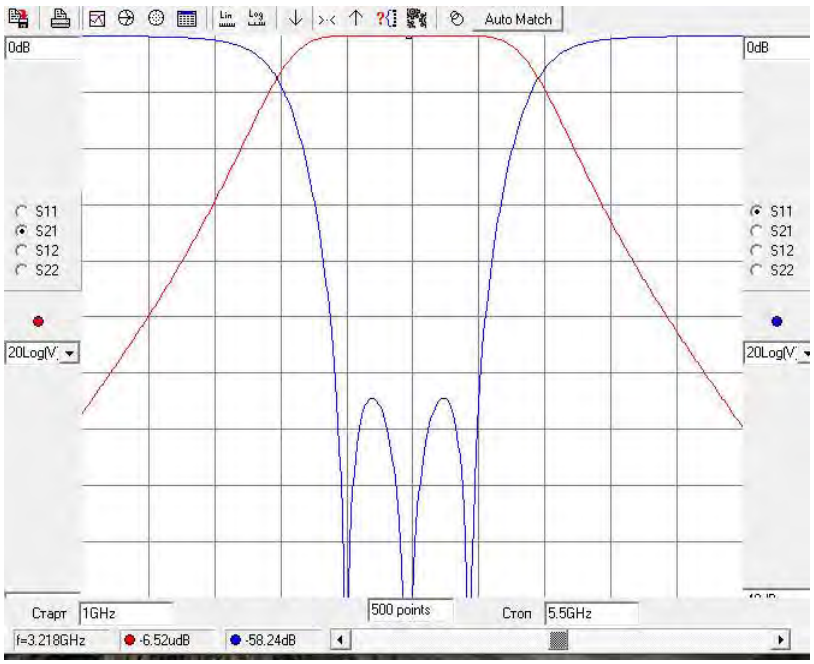


Рис. 9. АЧХ шлейфного полосового фильтра

Далее приступим к масштабированию. Меняем длины шлейфов и соединительных линий с одним и тем же коэффициентом подобия. Проследим за «движением» центральной частоты и шириной полосы пропускания, результаты представлены в таблице.

ТАБЛИЦА. Масштабирование длины шлейфов фильтра

	f_1, ГГц	f_2, ГГц	Δf		f_0, ГГц
			ГГц	%	
1:1	2,326	4,102	1,776	28	3,2
1:1,1	2,11	3,737	1,627	28	2,9
1:1,2	1,935	3,422	1,513	28	2,685
1:1,3	1,7888	3,155	1,367	28	2,475
1:1,4	1,661	2,931	1,27	28	2,286
1:1,5	1,549	2,734	1,185	28	2,145

Исходя из таблицы видно, что при изменении длины шлейфов меняется только центральная частота фильтра, ширина полосы пропускания остаётся прежней.

Здесь можно однозначно утверждать следующее:

– в результате изменения геометрических размеров топологии фильтра в различных соотношениях, центральная частота и ширина полосы пропускания изменяется по определённому закону;

– изменения геометрических размеров топологии в определенных соотношениях приводит к изменению АЧХ устройства, но сохраняет функционал фильтра;

– центральная частота, частота среза, крутизна, пульсации в полосе пропускания масштабируются на частотной оси однозначно и детерминировано в зависимости от коэффициента подобия.

Список используемых источников

1. Маттей Д. Л., Янг Л., Джонс Е. М. Фильтры СВЧ, согласующие цепи и цепи связи : пер. с англ. / под общ. ред. Л. В. Алексеева и Ф. В. Кушнира. М.: Связь, 1971. Т. 1. 349 с.

2. Булатова И. А., Иванова Е. А., Крюков А. Н., Седышев Э. Ю. Шлейфные фильтры СВЧ в объемном интегральном исполнении // Электроника и микроэлектроника СВЧ. 2016. С. 169–174.

3. Шомин А. Ю. Расчет фильтра Чебышева 3 порядка на резонаторах одинаковой длины: курсовая работа по дисциплине КМ ОИС СВЧ : курсовая работа / проверил Э. Ю. Седышев; СПбГУТ. СПб., 2020.

УДК 621.385.69
ГРНТИ 47.45.99

ТОЧНЫЙ СИНТЕЗ КОНСТРУКТИВНЫХ ИНДУКТИВНОСТЕЙ ИНТЕГРАЛЬНЫХ СХЕМ СВЧ

А. М. Румянцева, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе выполнен анализ математического аппарата синтеза индуктивностей для интегральных схем СВЧ. Рассмотрены различные методики синтеза круглых спиральных индуктивностей и алгоритмы их расчета. Исследовано влияние на номинал индуктивности паразитных параметров. Произведено сравнение методик между собой, а также сравнение результата расчёта с результатом эксперимента. Эксперимент проведен с использованием различных методов оценки реактивностей.

интегральные схемы, сверхвысокие частоты, плоские спиральные индуктивности, паразитные параметры, квазидинамическое приближение.

В современных интегральных схемах (ИС) сверхвысоких частот (СВЧ) широкое применение находят конструктивные индуктивности. В СВЧ схемах индуктивности могут быть выполнены в виде круглой спирали, квадратной, меандра, нити и др.

Спиральные индуктивности используются для уменьшения площади ИС. При изготовлении индуктивных элементов важно иметь высокую разрешающую способность технологического процесса, а также выбрать наиболее точную методику расчёта для получения точного номинала индуктивности с конкретной геометрии в требуемом частотном диапазоне.

При выборе инженерного метода синтеза круглых индуктивных элементов постоянно возникают трудности в выборе методик расчёта, так как описание каждой методики требует отдельного исследования. Следовательно, выбор методики синтеза и расчёта круглых спиральных индуктивностей с требуемой точностью в необходимом диапазоне является актуальной задачей.

При расчёте спиральной индуктивности (рис. 1) используются такие параметры как: число витков (*N*), внутренний диаметр (*D1*), внешний диаметр (*D2*), ширина спирали (*B*), расстояние между витками (*t*), чертёж с указанными параметрами представлен на рис. 2.

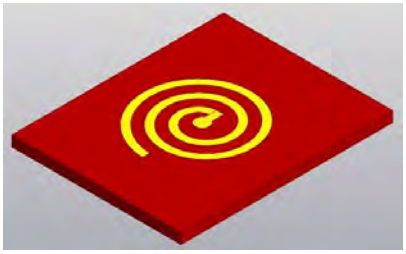


Рис. 1. 3D-модель планарной круговой индуктивности

Для оценки точности методик расчёта был изготовлен макет (рис. 2), содержащий планарную индуктивность с перемычкой и две контактные площадки (рис. 3). Изготовленная планарная индуктивность имеет следующие параметры: число витков 2,5, внешний диаметр 6 мм, внутренний диаметр 4 мм, расстояние между витками 0,5 мм, ширина токонесущей части 0,5 мм.

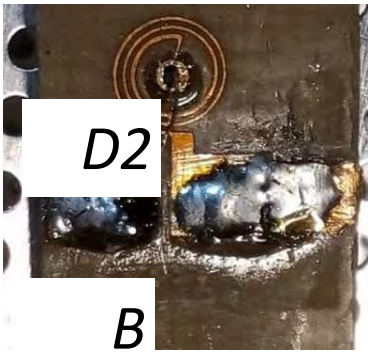


Рис. 2. Исследуемый макет

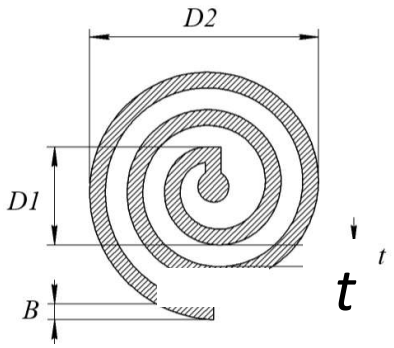


Рис. 2. Чертёж планарной круговой индуктивности и исследуемый макет

В предыдущей работе [1] были собраны и упорядочены формулы расчёта плоских спиральных индуктивностей различных инженерных методик. Оценка точности этих методик производилась квазистатическим методом. Для дальнейшего исследования выбраны три методики расчёта индуктивностей [2, 3, 4]. В таблице 1 представлены выбранные формулы и результаты расчёта планарной индуктивности синтезированного макета.

ТАБЛИЦА 1. Формулы расчёта индуктивности

№	Формула индуктивности	Полученное значение, нГн
1	$L = 2{,}475 \cdot D\text{ср} \cdot \sqrt[3]{N^5} \cdot \lg\left(\frac{4 \cdot D\text{ср}}{b}\right)$, где $D\text{ср} = 0{,}5 \cdot (D2 + D1)$, $b = R2 - R1$, $R2 = 0{,}5 \cdot D2$, $R1 = 0{,}5 \cdot D1$	$L = 74{,}142$
2	$L = 4{,}978 \cdot a \cdot \sqrt[3]{N^5} \cdot \lg\left(\frac{8 \cdot a}{b}\right)$, где $a = 0{,}5 \cdot (R2 + R1)$	$L = 74{,}562$
3	$L = N^2 \cdot D\text{ср} \cdot [\ln\left(\frac{2{,}46}{\varphi}\right) + 0{,}2 \cdot \varphi^2]$, где $\varphi = \frac{D2-D1}{D2+D1}$	$L = 78{,}675$

В таблице используются следующие обозначения: $R2$ – внешний радиус, $R1$ – внутренний радиус, φ – коэффициент заполнения, $D\text{ср}$ – средний диаметр, a – средний радиус, b – ширина катушки.

В СВЧ диапазоне на работу устройства оказывают влияние паразитные параметры проводников и диэлектрической подложки. На рис. 4 представлена принципиальная схема макета с учётом паразитных параметров.

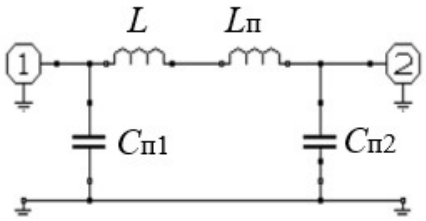


Рис. 4. Принципиальная схема колебательного контура, L – индуктивность, $L_\text{п}$ – паразитная индуктивность, $C_{\text{п}1}, C_{\text{п}2}$ – паразитные ёмкости

Перемычка планарной индуктивности также представляет собой индуктивность, которую можно рассчитать по формуле индуктивности одиночного прямолинейного круглого провода.

$$L_\text{п} = 2 \cdot l \cdot \left(\ln\frac{4l}{d} - 1\right) \cdot 10^{-9}, \quad (1)$$

где $L_\text{п}$ – индуктивность одиночного прямолинейного круглого провода,

l –длина провода,

d – диаметр провода.

В исследуемом макете перемычка имеет длину равную 7,5 мм и диаметр 0,02 мм.

По формуле (1) паразитная индуктивность составляет:

$$L_\text{п} = 2 \cdot 0{,}75 \cdot \left(\ln\frac{4 \cdot 0{,}75}{0{,}002} - 1\right) \cdot 10^{-9} = 9{,}47 \text{ нГн}.$$

Паразитные ёмкости рассчитываются по формуле плоского конденсатора (2).

$$C_{\text{п}} = \frac{\varepsilon_0 \varepsilon_r S}{h},$$

где $C_{\text{п}}$ – ёмкость плоского конденсатора,

ε_0 – электрическая постоянная,

ε_r – диэлектрическая проницаемость диэлектрика,

S – площадь пластины конденсатора,

h – высота подложки.

Как видно на рис. 3 в предложенном макете имеется две паразитные ёмкости, имеющие размеры (4×5) мм и (4×9) мм. Подложка выполнена из стеклотекстолита СТВЧ толщиной 1,5 мм с диэлектрической проницаемостью равной 5,5.

Расчёт паразитных ёмкостей даёт следующий результат:

$$C_{\text{п1}} = \frac{8{,}85 \cdot 10^{-12} \cdot 5{,}5 \cdot 4 \cdot 10^{-3} \cdot 5 \cdot 10^{-3}}{1{,}5 \cdot 10^{-3}} = 0{,}649 \text{ пФ},$$

$$C_{\text{п2}} = \frac{8{,}85 \cdot 10^{-12} \cdot 5{,}5 \cdot 4 \cdot 10^{-3} \cdot 9 \cdot 10^{-3}}{1{,}5 \cdot 10^{-3}} = 1{,}168 \text{ пФ}.$$

В результате проведённого эксперимента (рис. 5) получаем амплитудно-частотную характеристику (АЧХ) макета. Результаты эксперимента представлены на рис. 6.

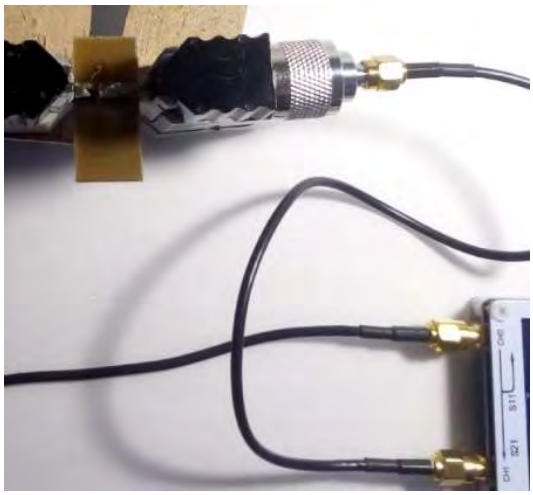


Рис. 5. Подключение исследуемого макета для снятия АЧХ

Следующим шагом нашего исследования было проведение эмуляции работы схемы в программе RFSimm. В первом этапе рассматривались значения индуктивностей, представленные в таблице 1 без учёта паразитных параметров. Во втором учитывались паразитные параметры с возможным разбросом значений на 25…40 %. В таблице 2 (см. ниже) представлено сравнение параметра S21 с результатами квазидинамического приближения. Полученная АЧХ при эмуляции представлена на рис. 7.

Рис. 6. Амплитудно-частотная характеристика макета, полученная в эксперименте

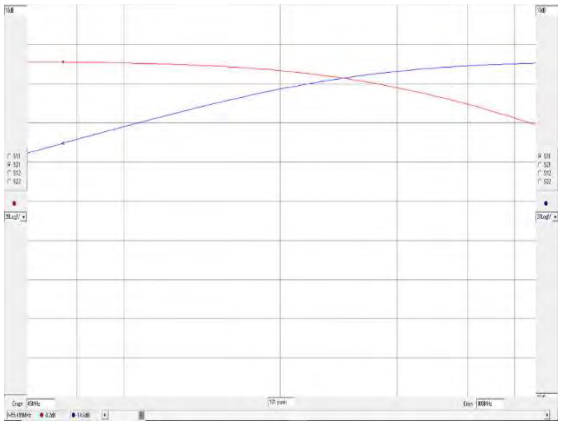


Рис. 7. Амплитудно-частотная характеристика макета в программе RFSimm

Как видно из таблицы 2 результаты, полученные в эксперименте и в программе RFSimm при варианте 2.6, имеют самые близкие значения. Полученные результаты показывают, что для исследуемого диапазона частот наиболее точна формула (1) с учётом паразитных параметров и разбросом значений 40 %.

Для получения более высокой точности расчёта необходимо увеличить частотный диапазон исследования, а также уменьшить зависимость передаточной характеристики от паразитных элементов (увеличить номинал исследуемой индуктивности).

ТАБЛИЦА 2. Результаты квазидинамического приближения

f, МГц	Эксперимент	Результаты, полученные в программе RFSimm								
		1.1	1.2	1.3	2.1	2.2	2.3	2.4	2.5	2.6
	S21, dB	S21, dB	S21, dB	S21, dB	S21, dB	S21, Db	S21, Db	S21, dB	S21, dB	S21, dB
45	–0,24	–0,19	–0,19	–0,21	–0,21	–0,22	–0,21	–0,32	–0,13	–0,09
90	–0,42	–0,71	–0,71	–0,78	–0,79	–0,82	–0,77	–1,16	–0,48	–0,35
207	–1,14	–2,9	–3,10	–3,11	–3,15	–3,23	–3,07	–4,19	–2,11	–1,63
288	–2,84	–4,47	–4,51	–4,81	–4,88	–5	–4,77	–6,2	–3,46	–2,77
360	–3,51	–5,87	–5,59	–6,2	–6,31	–6,46	–6,17	–7,78	–4,66	–3,84
486	–5,55	–7,87	–7,91	–8,31	–8,51	–8,72	–8,23	–10,12	–6,6	–5,68
594	–7,98	–9,39	–9,42	–9,83	–10,13	–10,39	–9,89	–11,8	–8,1	–7,16
720	–7,64	–10,85	–10,93	–11,96	–11,78	–12,12	–11,48	–13,5	–9,67	–8,78

f, МГц	Эксперимент	Результаты, полученные в программе RFSimm								
		1.1	1.2	1.3	2.1	2.2	2.3	2.4	2.5	2.6
	S21, dB	S21, dB	S21, dB	S21, dB	S21, dB	S21, Db	S21, Db	S21, dB	S21, dB	S21, dB
819	–11,2	–11,92	–11,96	–12,4	–12,94	–13,35	–12,6	–14,7	–10,79	–9,97

Варианты с уточнением параметров цепи для каждого этапа при эмуляции в САПР RFSimm:

1.1 – L = 74,142 нГн;

1.2 – L = 74,562 нГн;

1.3 – L = 78,675 нГн;

2.1 – L = 74,142 нГн, $L_{\text{п}}$, $C_{\text{п1}}$, $C_{\text{п2}}$;

2.2 – L = 74,142 нГн, $L_{\text{п}}$ + 25 %, $C_{\text{п1}}$ + 25 %, $C_{\text{п2}}$ + 25 %;

2.3 – L = 74,142 нГн, $L_{\text{п}}$ – 25%, $C_{\text{п1}}$ – 25 %, $C_{\text{п2}}$ – 25 %;

2.4 – L = 74,142 нГн + 25 %, $L_{\text{п}}$, $C_{\text{п1}}$, $C_{\text{п2}}$;

2.5 – L = 74,142 нГн – 25 %, $L_{\text{п}}$, $C_{\text{п1}}$, $C_{\text{п2}}$;

2.6 – L = 74,142 нГн – 40 %, $L_{\text{п}}$ + 40 %, $C_{\text{п1}}$ + 40 %, $C_{\text{п2}}$ + + 40 %;

Список используемых источников

1. Бочаров Е. И., Румянцева А. М., Седышев Э. Ю. Сравнение методов расчета конструктивных индуктивностей интегральных схем СВЧ // Региональная научно-методическая конференция магистрантов и их руководителей : сб. лучших докладов конф. / Сост. Н. Н. Иванов. СПб.: СПбГУТ, 2021. С. 330–334.

2. Скрипников Ю. Ф. Колебательный контур. М. : Энергия, 1970.128 с.

3. Торгонский Л. А. Проектирование интегральных микросхем и микропроцессов: учеб. пособие в 3-х разделах. Раздел 2. Томск : ТУСУР, 2011. 228 с.

4. Sunderarajan S. Mohan, Maria del Mar Hershenson, Stephen P. Boyd, and Thomas H. Lee. Simple Accurate Expressions for Planar Spiral Inductances // IEEE Journal of Solid-State Circuits, vol. 34, no. 10, October 1999.

УДК 621.396.67
ГРНТИ 47.45.29

КОЛЬЦЕВОЙ ЭЛЛИПТИЧЕСКИЙ РЕЗОНАТОР В КАЧЕСТВЕ ИЗЛУЧАТЕЛЯ

Э. Ю. Седышев, Р. И. Соковых

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе рассматривается возможность использования кольцевого эллиптического резонатора в качестве излучателя с круговой поляризацией. Рассматриваются модели кольцевых излучателей, различные способы их питания. Созданы макеты примитивных излучателей, доказана возможность их питания микрополосковой линией. Проведен ряд экспериментов, оценены входные параметры макетов.

кольцевой резонатор, излучатель, эллиптическая поляризация.

Микрополосковые антенны пользуются заслуженной популярностью в радиоэлектронике, они нашли своё применение в системах радиосвязи, навигации, широко используются в радиоэлектронных системах доступа [1, 2, 3, 4].

На данный момент хорошо изучены спиральные структуры [5], они позволяют осуществлять приёмопередачу электромагнитных волн круговой поляризации в широком диапазоне частот. Однако, широкая полоса частот не всегда востребована. Задачей нашей работы является создание узкополосного излучателя с эллиптической поляризацией в планарном исполнении.

В литературе описан ряд кольцевых (рис. 1) структур, которые не нашли широкого применения ввиду использования в них стоячей волны, к таким структурам относятся генераторы СВЧ (рис. 2) [6, 7].

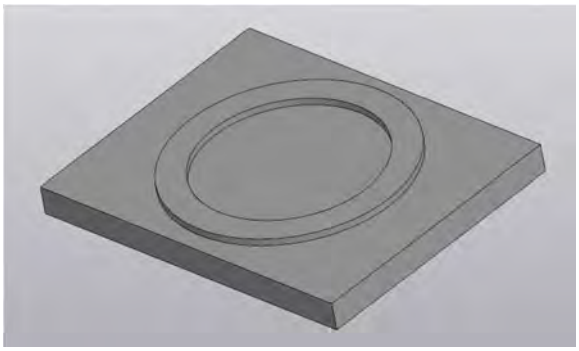
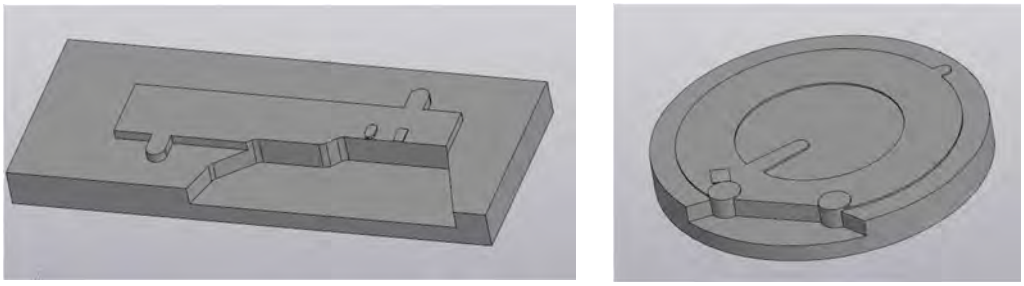


Рис. 1. Общий вид кольцевого резонатора

Структуры со стоячей волной по ряду технических характеристик проигрывают устройствам на бегущей волне, хотя геометрически они более компактны. Возьмем за основу структуру со стоячей волной и доработаем её до резонатора бегущей волны.



а) б)

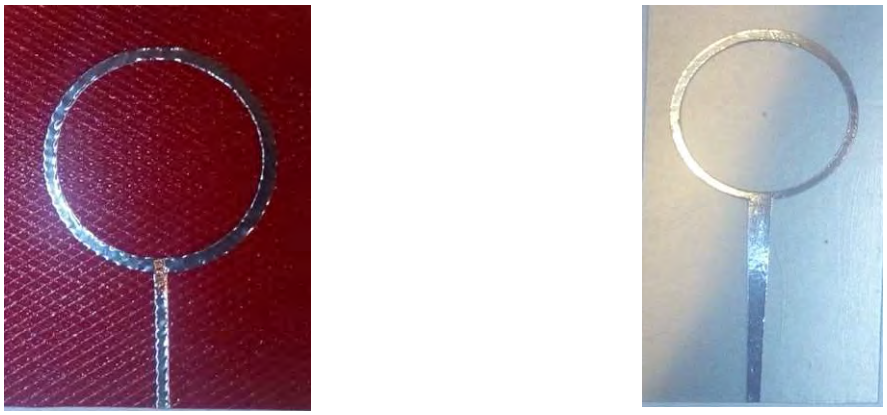
Рис. 2. Генераторы СВЧ на туннельных диодах:
а) с прямым полосковым резонатором, б) с кольцевым полосковым резонатором

Первым этапом работы было создание макета кольцевого резонатора на микрополосковой линии (рис. 3). Геометрия резонатора была выбрана с учётом собственной частоты резонатора, равной 2,5 ГГц (рис. 4). В результате эксперимента была получена характеристика КСВН с ярко выраженным резонансом на частоте 2,705 ГГц. Измерения показали, что рассчитанная и экспериментальная частота отличаются более чем на 200 МГц, что говорит о погрешностях при изготовлении макета и оценочном характере измерений.

Рис. 3. Кольцевой резонатор на микрополосковой линии

Рис. 4. КСВН кольцевого резонатора

Следующим этапом работы был синтезирован излучатель на основе кольцевого резонатора с использованием диэлектрической подложки из гофрированного полистирола (рис. 5, а). Данная структура имела одну резонансную частоту в диапазоне 1–4 ГГц, при этом была крайне неустойчива. Взяв диэлектрик с другими характеристиками, был изготовлен еще один макет излучателя на основе кольцевого эллиптического резонатора меньших размеров с элементами согласования. Второй излучатель использовал подложку из технического пенополипропилена. (рис. 5, б). Каждый излучатель был запитан микрополосковой линией.



а) б)

Рис. 5. Излучатель на основе кольцевого резонатора с использованием подложки: а) из гофрированного полистирола, б) из технического пенопропилена

На рис. 6 и 7 продемонстрирована работа кольцевого резонатора в качестве излучателя в диапазоне 1–4 ГГц. Эксперимент показал, что каждое кольцо имеет несколько резонансных частот, объяснить наличие нескольких близких по частоте резонансов одновременно на данный момент сложно. В кольцевой структуре бегущей волны имеются паразитные ёмкости и паразитные индуктивные, вносящие искажения в работу устройства. КСВН макета неудовлетворительный, но очевидно, что структура излучает электромагнитную волну. Самой близкой по природе излучения к нашему кольцевому резонатору является щелевая круговая антенна.

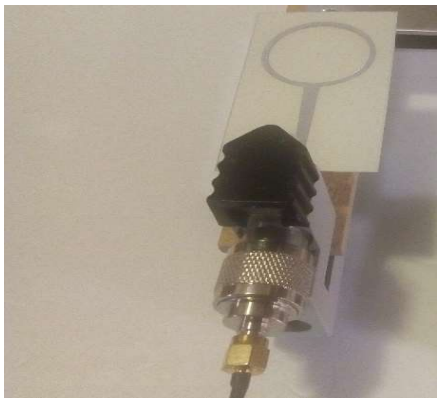


Рис. 6. Схема подключения излучателя

Рис. 7. Характеристики кольцевого резонатора в качестве излучателя

Завершающим этапом работы было создание кольцевого резонатора в качестве излучателя с использованием диэлектрической подложки из пенополиуретана и низким волновым сопротивлением (рис. 8). В результате эксперимента была получена осциллограмма резонанса (рис. 9) на частоте 1,399 ГГц с КСВН = 1,5.

Рис. 8. Кольцевой резонатор в качестве излучателя с подложкой из пенополиуретана

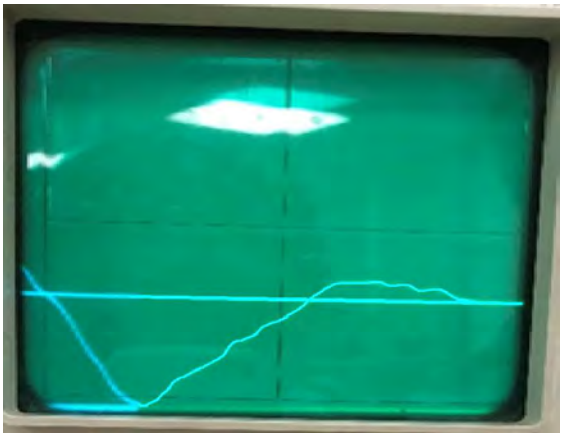


Рис. 9. КСВН кольцевого излучателя

Для данной структуры в программе RFSim99 была смоделирована приближенная эквивалентная схема (рис. 10) и получен график коэффициента S11 (рис. 11).

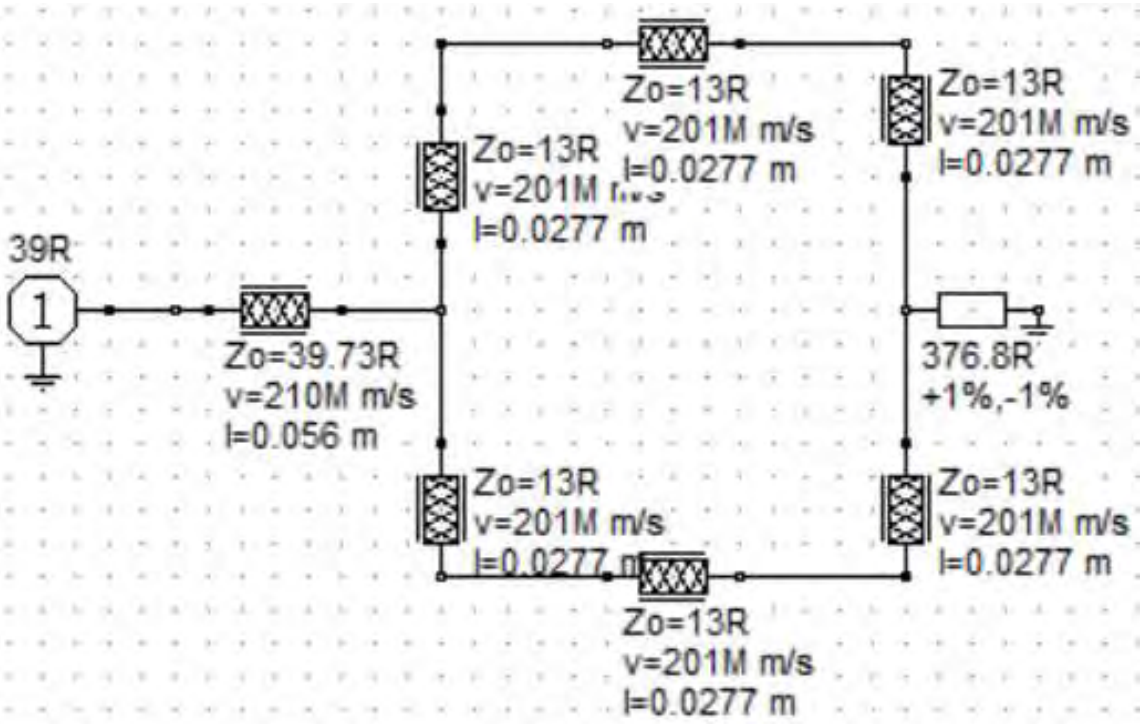


Рис. 10. Принципиальная схема макета

Таким образом, проведено исследование возможности использования кольцевого эллиптического резонатора в качестве излучателя. Рассмотрена возможность питания излучателя с помощью микрополосковой линии. В результате работы была получена структура кольцевого резонатора, работающая на излучение одной частоты.

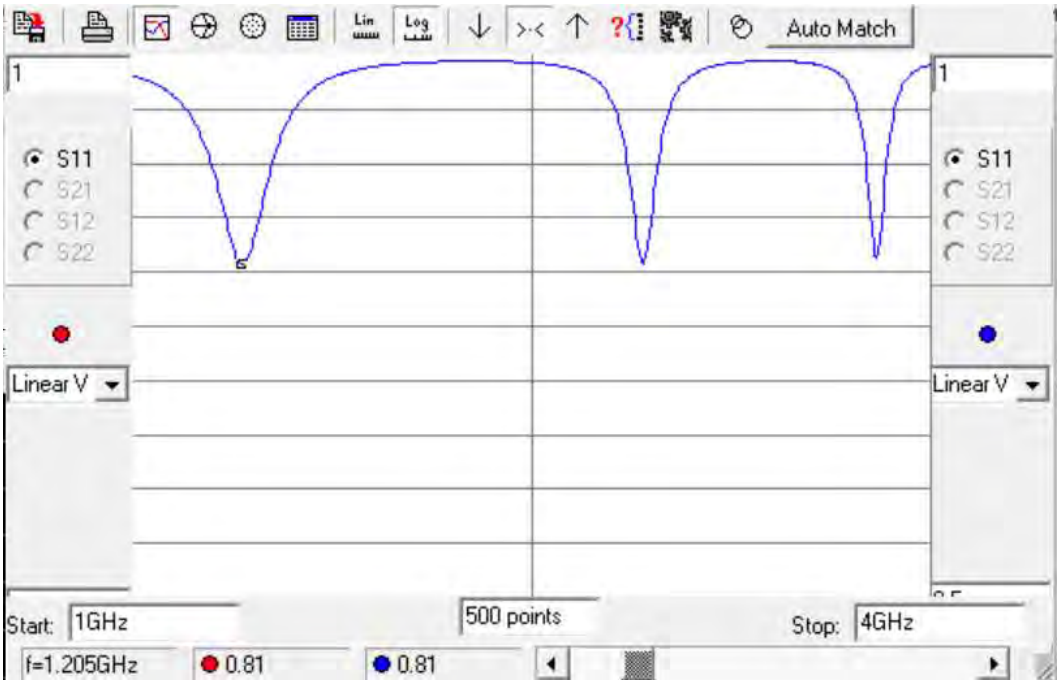


Рис. 11. Коэффициент S11

В ходе работы стало ясно, что характеристики кольцевого резонатора и, в частности, излучающая способность зависят, в основном, от волнового сопротивления токопроводящих элементов.

Список используемых источников

1. Фальковский О. И. Техническая электродинамика. М.: Связь, 1978. 431 с.

2. Папилов К. Б. Малогабаритные многослойные печатные антенны: дис. … канд. техн. наук : 05.12.07 / Папилов Константин Борисович. Москва, 2015. 170 с.

3. Безгин А. А., Савочкин А. А. Печатная антенна круговой поляризации Argos – 2 // Электроника и микроэлектроника СВЧ. Санкт-Петербург, 2015. С. 301–304.

4. Воскресенский Д. И., Овчинникова Е. В. и др. Широкополосная микроволновая антенна. Пат. RU157955U1 Российская Федерация; заявитель и патентообладатель Фед. гос. бюдж. обр. учрежд. высш. проф. обр-я Моск. авиационный ин-т. – № RU2014153321/08U; заявл. 29.12.2014; опубл. 20.12.2015.

5. Бочаров Е. И., Лепихин К. А., Седышев Э. Ю. Исследование спиральных структур с экраном // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. Т. 3. С. 404–407.

6. Янчук Е. В. Туннельные диоды в приемно-усилительных устройствах. М. : Энергия, 1967. 56 с.

7. Вольман В. И. Справочник по расчету и конструированию СВЧ полосковых устройств. М. : Радио и Связь, 1982. 326 с.

УДК 621.372.54
ГРНТИ 47.05.05

ОЦЕНКА ВЛИЯНИЯ ПОТЕРЬ В ЭЛЕМЕНТАХ LC-ФИЛЬТРА НА ХАРАКТЕРИСТИКУ ЗАТУХАНИЯ

В. В. Сергеев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Показано, что для классических реактивных фильтров нижних частот с согласованными нагрузками максимальное (в рабочей области) приращение затухания, обусловленное потерями в элементах, соответствует граничной частоте полосы пропускания и оценивается через максимальную суммарную реактивную энергию. Приведены простые соотношения для оценки влияние потерь на изменение неравномерности затухания в полосе пропускания фильтра.

реактивный фильтр, влияние потерь, энергетические функции.

При практической реализации LC-фильтров конденсаторы и катушки индуктивности могут иметь существенные активные потери энергии, которые будут изменять характеристики фильтра, рассчитанные без учета потерь.

Эквивалентная схема катушки индуктивности с потерями, используемая в большинстве случаев, представляется в виде последовательного соединения элемента индуктивности L_k и резистивного сопротивления R_k. Схему же реального конденсатора представляют в виде параллельного соединения емкости C_i и резистивной проводимости G_i.

Потери в элементах можно оценить по их добротностям или по коэффициентам потерь, которые определяются как величины обратные добротностям. Добротность катушки определяется по формуле $Q_k = (\omega_0 L_k) / R_k$, где R_k – активное сопротивление k-й катушки индуктивности, добротность конденсатора $Q_i = (\omega_0 C_i)/ G_i$, где G_i – активная проводимость i-го конденсатора. Частота ω_0 является граничной для полосы пропускания фильтра. При этом коэффициенты потерь (обратные добротности) $d_k = R_k / (\omega_0 L_k)$ (для катушки) и $d_i = G_i / (\omega_0 C_i)$ (для конденсатора).

В большинстве случаев рассматривают полуоднородные потери, когда для всех емкостей $d_i = d_C$ и для всех индуктивностей $d_k = d_L$. Это обусловлено с тем, что фильтрующие цепи, как правило, реализуются на однотипных элементах. Таким образом, с учетом потерь в элементах их комплексные сопротивления и проводимости (импедансы) получают некоторые малые приращения:

$Z_k = j\omega L_k + R_k = L_k\,(j\omega + \omega_0\, d_L)$ и $Y_i = j\omega\, C_i + G_i = C_i\,(j\omega + \omega_0\, d_C)$.

В дальнейшем будем предполагать, что при реализации фильтра обеспечиваются достаточно малые коэффициенты потерь элементов (не более 0,02–0,01), что почти всегда имеет место на практике.

Будем анализировать влияние потерь на частотные характеристики затухания и фазы. Для этого рассмотрим логарифмическую комплексную функцию передачи [1, 2]

$$\ln H(j\omega) = \ln[|H(j\omega)|\, e^{j\theta(\omega)}] = \ln|H(j\omega)| + j\theta(\omega). \qquad (1)$$

Первое слагаемое в (1) может быть выражено через функцию затухания $\ln|H(j\omega)| = -0{,}1151(20\lg|H(j\omega)|^{-1}) = -0{,}1151a(\omega)$. Таким образом, логарифмическая комплексная функция передачи имеет вещественную часть, связанную с затуханием и мнимую часть, равную ФЧХ. Эта функция будет зависеть от импедансов Z_k и Y_i. Эти импедансы, как было показано, определяются параметрами элементов и коэффициентами потерь. Поэтому полный дифференциал (малое приращение) рассматриваемой функции:

$$\mathrm{d}\ln H(j\omega) = \sum_{k=1}^{N_L} \frac{\partial \ln H(j\omega)}{\partial Z_k}\, dZ_k + \sum_{i=1}^{N_C} \frac{\partial \ln H(j\omega)}{\partial Y_i}\, dY_i. \qquad (2)$$

В правой части (2) перейдем к частным производным по параметрам L_k и C_i (то есть к параметрическим функциям чувствительности (ФЧ)) и учтем, что $dZ_k = \omega_0 L_k\, d_L$; $dY_i = \omega_0 C_i\, d_C$; и производные $\partial L_k / \partial Z_k = \partial C_i / \partial Y_i = 1/(j\omega)$. Поскольку в (2) входят идентичные слагаемые, рассмотрим преобразование одного из них с учетом (1):

$$\frac{\partial \ln H(j\omega)}{\partial Z_k}\, dZ_k = \frac{\partial \ln H(j\omega)}{\partial L_k} \cdot \frac{\omega_0 L_k d_L}{j\omega} = \frac{\omega_0 d_L}{j\omega}\left[-0{,}1151\frac{\partial a}{\partial L_k} L_k + j\frac{\partial \theta}{\partial L_k} L_k\right] =$$
$$= \frac{\omega_0 d_L}{\omega}\left[Q_k^{\theta}(\omega) + j0{,}1151 Q_k^{a}(\omega)\right].$$

Таким образом, каждое слагаемое в правой части (2) будет содержать вещественную (связанную с ФЧ ФЧХ – $Q_k^{\theta}(\omega)$)) и мнимую (связанную с ФЧ затухания – $Q_k^{a}(\omega)$) составляющие.

В левой части (2) произведем аналогичные преобразования и перейдем от дифференциала к конечным приращениям:

$$d\ln H(j\omega) \approx -0{,}1151 a_{\Pi}(\omega) + j\theta_{\Pi}(\omega),$$

где через $a_{\Pi}(\omega)$ и $\theta_{\Pi}(\omega)$ – обозначены приращения рабочего затухания и фазы, обусловленные влиянием потерь в элементах LC-фильтра.

После указанных преобразований приравниваем вещественные и мнимые составляющие в (2). Получим следующие приближенные соотношения для приращений функции затухания и ФЧХ за счет потерь в элементах:

$$a_{\Pi}(\omega) = -8{,}686\frac{\omega_0}{\omega}\left[d_L Q_L^{\theta}(\omega) + d_C Q_C^{\theta}(\omega)\right], \quad (3)$$

$$\theta_{\Pi}(\omega) = 0{,}1151\frac{\omega_0}{\omega}\left[d_L Q_L^{a}(\omega) + d_C Q_C^{a}(\omega)\right],$$

где $Q_L^a(\omega) = \sum_{k=1}^{N_L}\frac{\partial a(\omega)}{\partial L_k}L_k$; $Q_L^a(\omega) = \sum_{i=1}^{N_C}\frac{\partial a(\omega)}{\partial C_i}C_i$ – суммы полуотносительных ФЧ рабочего затухания по всем индуктивностям L_k (N_L – их число) и по всем емкостям C_i (N_C – их число) фильтра без потерь;

$Q_L^{\theta}(\omega)$ и $Q_C^{\theta}(\omega)$ – аналогичные суммы ФЧ ФЧХ. Затухание представлено в дБ.

Поскольку для фильтрующих цепей основной является характеристика затухания, то дальше будем рассматривать соотношение (3), то есть приращения рабочего затухания, обусловленные влиянием потерь в элементах.

Из [1] следует, что суммы ФЧ могут быть выражены через номинальные функции LC-фильтра на основании свойств инвариантности и через суммарные реактивные энергии. В частности, для симметричных и антиметричных реактивных фильтров, к которым относятся классические LC-фильтры, с достаточной степенью точности справедливы следующие соотношения:

$$Q_L^{\theta}(\omega) = Q_C^{\theta}(\omega) = -0{,}5\tau(\omega)\cdot\omega = -\frac{\omega\cdot W(\omega)}{4P_{2\max}}, \quad (4)$$

где $\tau(\omega) = -\frac{d\theta(\omega)}{d\omega}$ – функция групповой задержки (ГВЗ);

$W(\omega) = \sum_{i=1}^{N_C} U_i^2 C_i + \sum_{k=1}^{N_L} I_k^2 L_k$ – суммарная максимальная реактивная энергия по всем емкостям и по всем индуктивностям;

$P_{2\max} = U_1^2/4R_1$ – максимальная мощность, которая может быть передана от источника U_1 с сопротивлением R_1 в нагрузку.

Подставляя (4) в (3), получим:

$$a_{\Pi}(\omega) = 8{,}686 d_{LC}\cdot\omega_0\tau(\omega) = 4{,}343\, d_{LC}\cdot\frac{\omega_0\cdot W(\omega)}{P_{2\max}}, \quad (5)$$

где $d_{LC} = 0{,}5(d_L + d_C)$ – суммарный коэффициент потерь.

Согласно полученным соотношениям приращения затухания и ФЧХ, обусловленные потерями в элементах, зависят не только от коэффициентов потерь, но и от свойств функций фильтра, а именно функции ГВЗ или сум-

марной реактивной энергии. Указанные функции имеют максимальные значения, как правило, на граничной частоте, поэтому (5) целесообразно рассматривать при $\omega = \omega_0$, что будет соответствовать максимальному приращению затухания в рабочей области (в полосе пропускания).

Функция ГВЗ, входящая в (5), для некоторых случаев приведена в справочниках или может быть легко рассчитана по справочным данным. Заметим, что $\omega_0 \cdot \tau(\omega) = \tau(\Omega)$ – нормированная функция ГВЗ при $\Omega = \omega/\omega_0$.

Отметим, что суммарная реактивная энергия является универсальным показателем эффективности LC-фильтров и определяет массу, габаритные размеры, КПД и стабильность характеристик фильтра. Согласно (5) к перечисленным показателям можно добавить и степень влияния потерь на характеристику затухания. В [1] рассмотрены методы минимизации реактивной энергии и оптимизации указанных показателей эффективности реактивных фильтров.

Известно, что к влиянию потерь наиболее чувствительным параметром является неравномерность Δa характеристики затухания в полосе пропускания фильтра. Потери в элементах могут существенно увеличить Δa по сравнению с расчетным значением. Соотношение (5) дает возможность оценить влияние потерь на изменение неравномерности затухания в полосе пропускания.

Необходимо отметить, что соотношения (3)–(5) являются приближенными, но как было отмечено выше, выполняются с достаточной для практики точностью.

В качестве примера проанализируем влияния потерь в элементах LC-фильтра нижних частот (ФНЧ) Чебышева, у которого порядок $n = 7$ и неравномерность затухания в полосе пропускания $\Delta a = 0{,}1$ дБ. Предположим, что коэффициенты потерь в элементах $d_L = 0{,}005$ (добротность 200) и $d_C = 0{,}002$ (добротность 500). Расчетным путем для указанного ФНЧ получено максимальное (на граничной частоте полосы пропускания) значение относительной суммарной реактивной энергии $\hat{W} = \omega_0 W_{max} / P_{2max} = 27{,}56$. Подставляя приведенные данные в (5), получим приращение затухания $a_П = 0{,}4189$ дБ. Это приращение затухания соответствует граничной частоте полосы пропускания и обусловлено потерями в элементах LC-фильтра.

Для проверки степени точности полученного результата было проведено моделирование на ЭВМ рассматриваемого ФНЧ с учетом заданных коэффициентов потерь.

Результаты моделирования приведены на рис. в виде графиков функции рабочего затухания в полосе пропускания с учетом и без учета потерь.

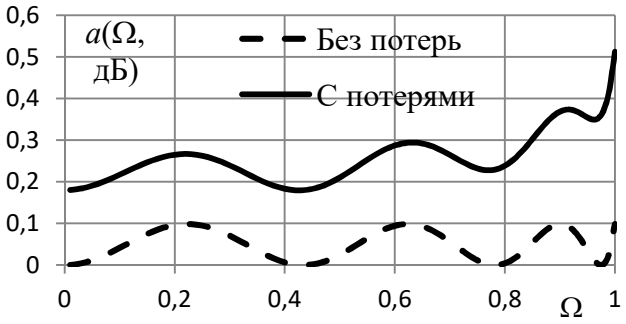


Рис. Характеристики затухания ФНЧ Чебышева (n = 7, Δa = 0,1 дБ)

По результатам моделирования приращение затухания $a_П$ вычисляется при Ω = 1 как разность двух значений затухания – одно с учетом потерь (0,5125 дБ) другое – без учета потерь (то есть номинальное 0,1 дБ). Получаем $a_П$ = 0,4125, что практически совпадает с ранее вычисленным значением по (5).

Полученное соотношение (5) может быть также использовано для оценки требуемых коэффициентов потерь (добротностей) элементов по заданному допустимому приращению затухания в полосе пропускания фильтра.

Для примера рассмотрим тот же ФНЧ Чебышева порядка n = 7 и с неравномерностью затухания в полосе пропускания Δa = 0,1 дБ. Предположим, что допустимое увеличение затухания в рабочей области составляет $a_П$ = 0,4 дБ. Тогда, согласно (5) при $\omega_0 W_{max} / P_{2max}$ = 27,56, допустимый коэффициент потерь $d_{LC} = 0{,}5(d_L + d_C) = 0,\ 00167$. Можно принять d_C = 0,00067 (добротность 1 490) и d_L = 0,001 (добротность 1 000), что вряд ли реализуемо на практике.

В заключение отметим, что методы, изложенные в [1], позволяют в некоторых случаях в несколько раз уменьшить максимальную реактивную энергию фильтра при прочих равных условиях, что приведет и к снижению степени влияния потерь на характеристику затухания.

Список используемых источников

1. Дмитриков В. Ф., Сергеев В. В., Самылин И. Н. Повышение эффективности преобразовательных и радиотехнических устройств. 2-е изд., стереотип. М.: Горячая линия – Телеком, 2016. 424 с.

2. Трифонов И. И. Расчет электронных цепей с заданными частотными характеристиками. М.: Радио и связь, 1988. 304 с.

УДК 621.375.026
ГРНТИ 47.41.33

РАЗРАБОТКА КОМПЬЮТЕРНОЙ МОДЕЛИ И ИССЛЕДОВАНИЕ ТРАНЗИСТОРНОГО СВЧ УСИЛИТЕЛЯ ПО СХЕМЕ ДОГЕРТИ

Э. Сурков, В. А. Филин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Описан механизм работы усилителя мощности по схеме У. Догерти. Создана модель данного усилителя в программе Fastmean с использованием кусочно-линейной схемы замещения мощных GaN-транзисторов. Модель рассчитана на усиление модулированного сигнала с центральной частотой 500 МГц. Получены значения мощностей и КПД усилителя, произведено сравнение с усилителями, работающими в режимах АВ и С.

усилитель мощности, Догерти, Fastmean. транзисторный СВЧ усилитель, усилитель класса АВ, усилитель класса С.

В 1936 году Уильямом Догерти была предложена схема повышения КПД лампового усилителя мощности амплитудно-модулированного (АМ) сигнала, работающего в режиме АВ. В последние годы с ростом исследований и разработок в области интегральных усилителей мощности СВЧ диапазона, вновь проявляется повышенный интерес к энергетически эффективным схемотехническим решениям. В данной работе схема Догерти рассматривается в качестве одного из перспективных решений.

Идея усилителя заключается в построении двух каналов усиления: основного усилителя класса АВ и вспомогательного усилителя класса С. Этим достигается «дополнение» формы выходного сигнала усилителем С (далее пиковым) при увеличении амплитуды сигнала и приближении усилителя АВ (далее основного) к режиму насыщения, тем самым сохраняя форму сигнала на выходе неискажённой. На рис. 1 представлена структурная схема данного усилителя, содержащая помимо самих усилителей несколько важных для её корректной работы элементов.

Принцип работы устройства отличается способом разделения и объединения выходов усилителей таким образом, что ветви усилителей работают не перегружая друг друга, т. е. пиковый усилитель не нагружает верхнюю ветвь при работе основного усилителя и наоборот, при насыщении основного усилителя не нагружается нижняя ветвь устройства [1].

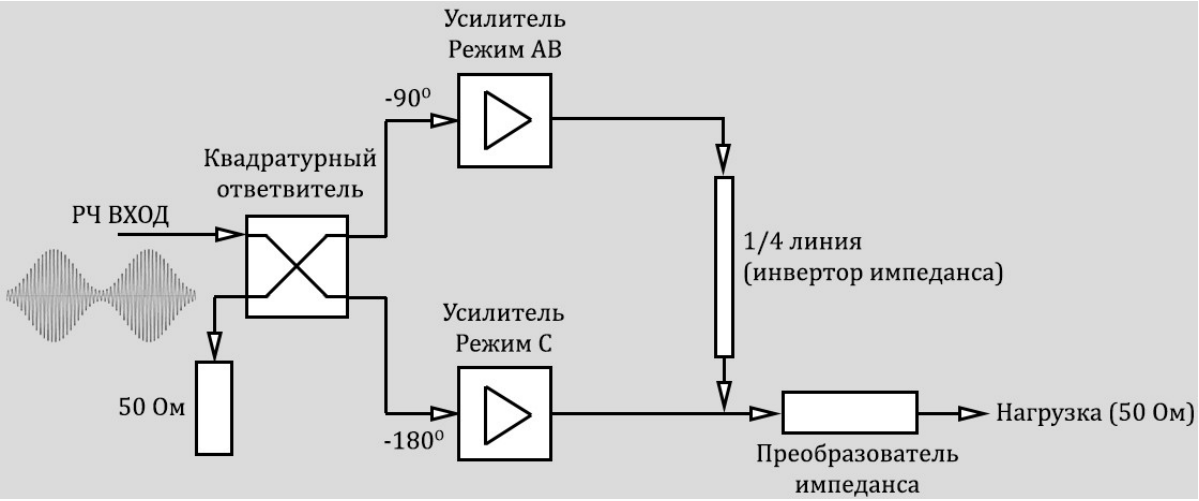


Рис. 1. Структурная схема усилителя Догерти

По данной схеме была создана модель в программе моделирования электрических цепей Fastmean (рис. 2) [2].

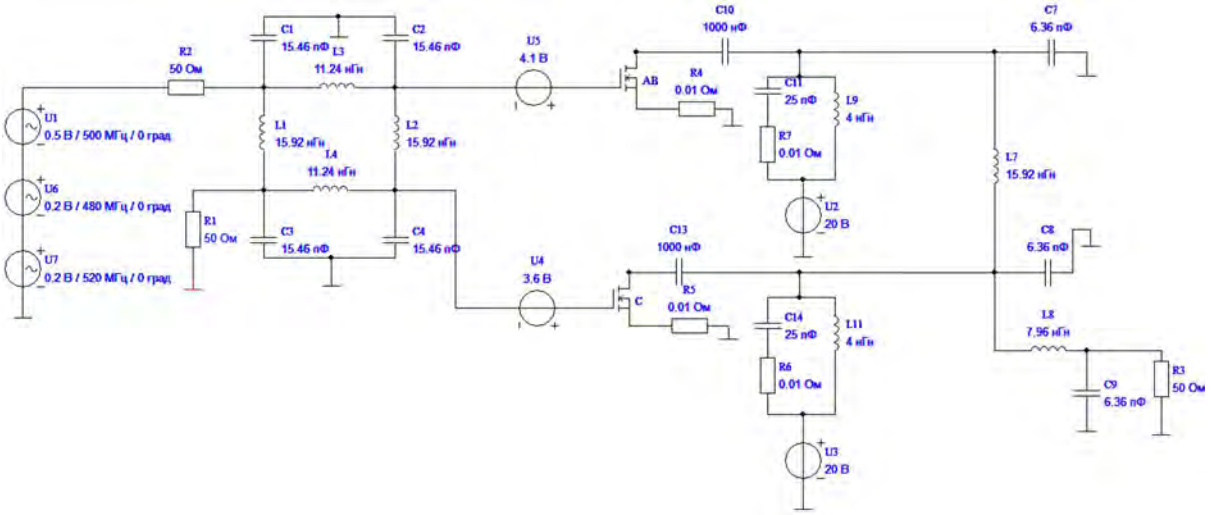


Рис. 2. Компьютерная модель усилителя Догерти в программе Fastmean

Схема рассчитана на несущую частоту входного АМ сигнала 500 МГц и диапазон рабочих частот 480–520 МГц.

Далее в модели расположен квадратурный мост, который служит для разделения входного сигнала на два одинаковой амплитуды со сдвигом фаз 90 градусов. Это необходимо для компенсации набега фазы на инверторе импеданса, чью роль выполняет четвертьволновая линия. При этом использование квадратурного моста позволяет достичь согласования по входу путём направления любой отражённой мощности в нагрузку изолированного порта, а не в источник [1].

Нитрид-галлиевые (GaN) полевые транзисторы, используемые в качестве усилителей в данной схеме, описываются кусочно-линейной моделью [3], способной воспроизводить режимы отсечки, насыщения и активного режима (рис. 3).

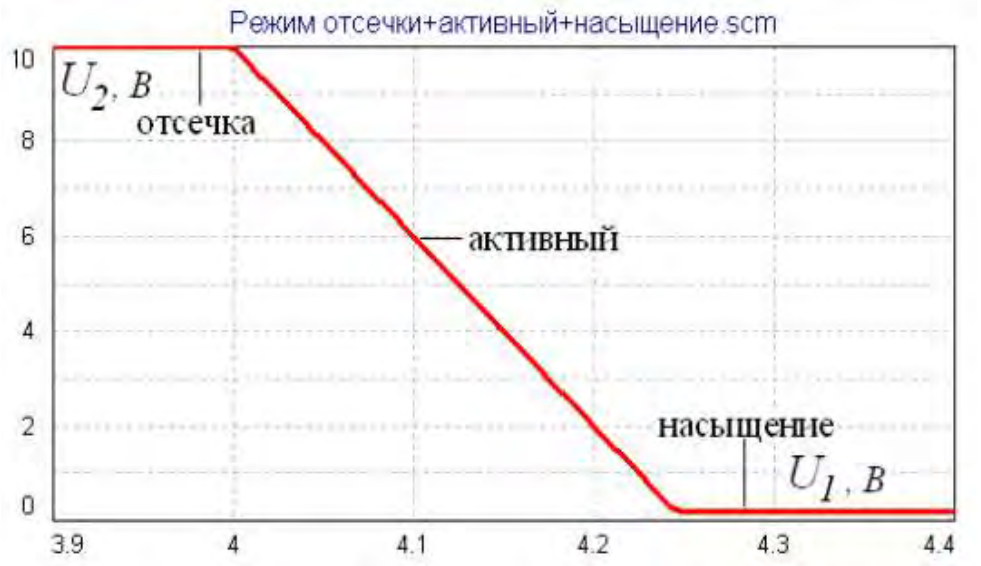


Рис. 3. Статическая передаточная характеристика типового GaN-транзистора

На выходах усилителей размещены фильтры гармоник, а также эквивалентное LC-звено четвертьволновой линии (инвертора импеданса), соединяющее выходы усилителей и в сочетании с преобразователем импеданса на выходе схемы, обеспечивающее эффект «модуляции импеданса» на выходе основного усилителя. Благодаря этому эффекту обеспечивается высокий КПД данной схемы, поскольку рост тока основного усилителя увеличивает результирующую выходную мощность [4].

В результате моделирования были получены значения средней потребляемой от источника питания и полезной выходной мощностей посредством использования в программе функции усреднения по времени (*average – avg*) мгновенных значений тока через транзистор и напряжения в нагрузке для установившегося режима: P_O = 6,34 Вт и $P_Н$ = 3,15 Вт. Средний КПД схемы Догерти составил 49,69 %. Для сравнения были получены значения мощностей и КПД усилителей, входящих в схему Догерти и работающих в режимах АВ и С с минимальным и максимальным уровнем входного возбуждения (рис. 4, 5). В режиме АВ максимальный КПД составил 55 %, а минимальный – 20 %. В режиме С максимальный КПД – 85 %, минимальный – 28 %. Таким образом средний КПД в режиме АВ составил 37,5 %, в режиме С – 56,5 %.

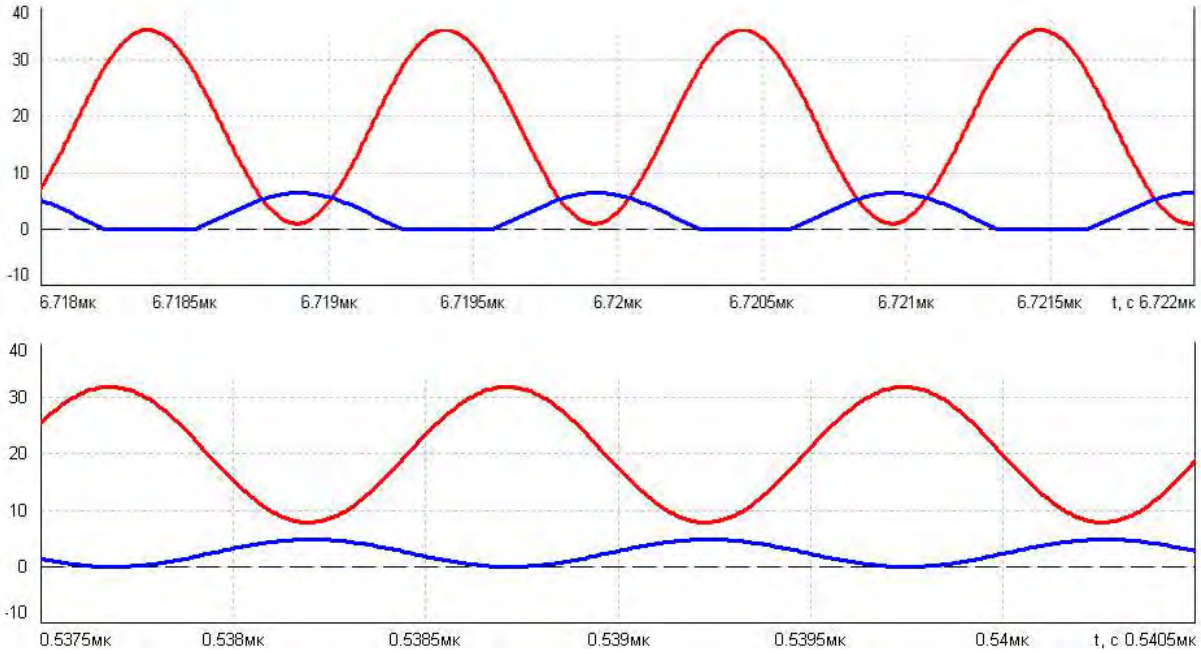


Рис. 4. Выходное напряжение и ток через транзистор усилителя в режиме АВ с максимальной и минимальной амплитудой возбуждения.

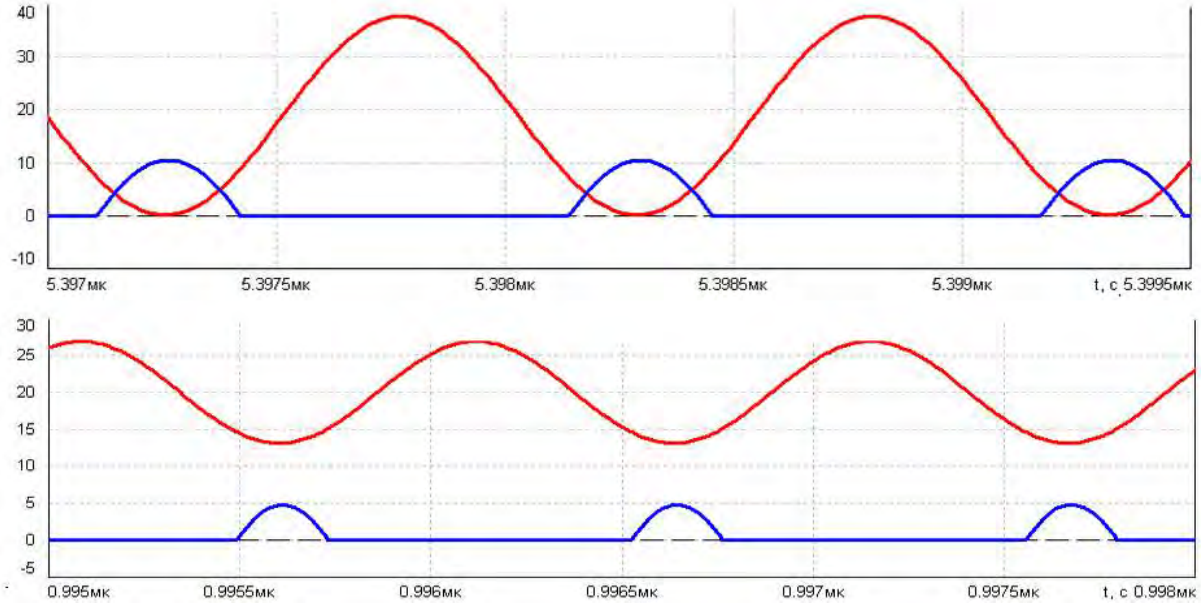


Рис. 5. Выходное напряжение и ток через транзистор усилителя в режиме С с максимальной и минимальной амплитудой возбуждения.

Анализируя результаты моделирования можно утверждать, что схема Догерти за счет введения дополнительного (пикового) усилителя повышает средний КПД усилителя по сравнению с режимом АВ на 12–15 %, сохраняя линейность усиливаемого сигнала при больших его уровнях на входе. Однако данная схема требует тщательной настройки с целью обеспечения необходимых амплитудных и фазовых соотношений между сигналами.

Список используемых источников

1. Slade B. The Basics of the Doherty Amplifier. URL: http://orbanmicrowave.com/the-basics-of-power-amplifiers-part3/ (дата обращения 28.03.2021).

2. FASTMEAN. URL: https://www.fastmean.ru (дата обращения 28.03.2021).

3. Ганбаев А. А., Филин В. А. Упрощенная динамическая модель мощных полевых транзисторов для исследования ключевых режимов радиочастотных устройств // Труды учебных заведений связи. 2019. Т. 5. № 2. С. 66–75.

4. Косичкина Т., Кочемасов В. Усилители мощности по схеме Догерти // Электроника. 2019. № 3. С. 144–152.

A N N O T A T I O N S

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Avnigina A., Fedorova A. Informatization of Time-Management in Automation of Road Digital Displays. – PP. 5–9.
The article gives the concept of road digital displays of variable information, the ways of their attachment and additional elements. Variable information displays are compared with dynamic information displays in terms of technical characteristics. The necessity of using time management is substantiated. The ways of its informatization in the process of automation of road digital displays are proposed.
Key words: time-management, control, time, traffic board, road signs, variable information board, road sensors, information systems.

Avramenko V., Malikov A. Evaluation of Efficiency of the Diagnosing of Computer Incidents in Infocommunication Systems. – PP. 10–15.
The article discusses the approach to assessing the effectiveness of diagnosing of computer incidents in infocommunication systems. Performance indicators and their evaluation procedure are presented. The focus is on evaluating the effectiveness of computer incident diagnosis systems using artificial neural networks.
Key words: computer incident, efficiency, indicator, assessment, artificial neural networks.

Aduevskiy A., Kucherevskiy K., Savin M., Soloviev D. Artificial Neural Networks in the Detection of Low-Intensity Denial-of-Service Attacks on an Information System. – PP. 15–19.
This article discusses modern network threats and DoS and DDoS attacks. The most common network threat at the moment is a low intensity DDoS attack. To predict and detect these attacks, security systems using artificial neural networks (ANNs) are used. This method is the most effective, since ANNs are able to learn in the process of work in real time.
Key words: attack detection, DoS attack, DDoS attack, low intensity DDoS attack, artificial neural network.

Aduevskiy A., Kucherevsky K., Savin M., Soloviev D. Parametric Optimization of a Complex Optical Fiber Drawing Process. – PP. 19–22.
This article shows a method for solving a CAD optimization problem using artificial neural network technologies using the example of parametric optimization of the technological process of pulling an optical fiber.

Key words: computer-aided design systems, artificial neural networks, software, optical fiber, multilayer perceptron.

Akimov S., Davletshina E. Models of Human Resource Management in the Cyber Environment of Virtual Enterprises. – PP. 23–27.
Virtual enterprises and organizations are now becoming more and more widespread, thanks to the ability to flexibly manage the process of combining the resources of various partners to solve a specific problem. The technology of virtual enterprises and organizations allows, in the shortest possible time, to create geographically distributed temporary labor collectives according to specified criteria for their participants. The article presents the results of the development of models of human resource management in the cyber environment of virtual enterprises and organizations based on an electronic portfolio, automatic calculation of ratings and the degree of compliance of the solved problem by both individuals and work collectives.
Key words: cyber environment, virtual enterprises, e-portfolio, automation, Industry 4.0.

Andrianova E., Lipanova I. Ways to Ensure Data Security in Oracle SQL Developer. – PP. 28–32.
In modern business, and in general, in all areas of human activity, data security is given a special place. Each organization must ensure the safety of the data available in it. The report discusses two ways to ensure data security in the Oracle SQL Developer relational database development environment. The first method is provided by restricting the user's rights when assigning Grant casts. The second method is to create views that you can use to restrict access to a specific table. The report provides examples of the implementation of these methods.
Key words: databases, data security, Oracle SQL Developer, relational database, access rights.

Anikieva A., Gunina E. Virtual Tours Based on 3d Technologies. – PP. 33–36.
This article introduces the process of combining virtual tours and 3D models. The stages of the development of 3D models, with their subsequent implementation into spherical panoramas, are described. Particular attention is paid to the relevance of 3D panoramas in various fields of activity. Today virtual tours are popular among construction companies, architectural firms and advertising agencies. Also, ideas were formulated for further development of the use of 3D technologies in the creation of virtual tours.
Key words: virtual tours, 3D, modeling, graphics, 3D-model, VR, AR, MR, visualization.

Antonov V. Application of Containerization in the Framework of Teaching Technical Courses. – PP. 36–41.
The software options for the implementation of containers are considered. The description of creating images for containers is given. Options for configuring containers for use in practical and laboratory work in various technical disciplines are proposed. The prospects of using containerization for building and studying the technological stack of microservice architectures are disclosed.
Key words: virtualization, containers, images, Docker, microservices.

Arkhipov M., Markin D. Algorithm for Detecting Harmful Shell Codes Based on Static Heuristic Characteristics. – PP. 41–46.
The article describes an algorithm for detecting shellcodes based on static heuristic features for computer systems based on processors with the ARM architecture. Described is a software tool developed to demonstrate the operation of the algorithm, its structure, test data for evaluating efficiency, and a malware model for ARM systems.
Key words: polymorphic code, ARM, shellcode, detection, signature, heuristic features.

Arkhipova M., **Fedorova A.** Research of Game Optimization Methods in Cross-Platform Development Environments (Using the Example of Unity). – PP. 47–49.
The article is devoted to the consideration of various methods of optimizing games developed using the Unity software. In the process of creating games, the issue of ensuring a high level of their performance on various devices becomes relevant. The optimization task is to get the maximum performance gain with the minimum amount of resources spent. The main methods of solving this problem will be considered, and their features will be identified, allowing them to be used in the implementation of projects in the Unity development environment. A number of recommendations will also be offered to help improve the optimization of games created using the cross-platform development environment under consideration.
Key words: unity, game optimization, FPS, cashing, static batching, dynamic batching.

Akhmetshina M., Mankaev R., Ushakov A. Audit of Information Security of Organizations using Network Analyzers and Penetration Tests. – PP. 50–55.
The modern world can no longer be imagined without gadgets, fast Internet access and other modern devices that people are used to using every day. They become indispensable attributes of our life that accompany a person in everyday life: both at home and at the workplace. All processes in modern society flow into information systems, which play a central role in ensuring the efficiency of commercial, state-owned enterprises and educational organizations. The widespread use of information systems, which are used for storing, processing and transmitting information, determines the relevance of the problem of protecting and preserving information in them.
Key words: information security audit, sniffers, network traffic, Snort.

Babaeva A., Litvinov V. Application of Methods of Artificial Intelligence in Forecasting Financial State Credit Organizations. – PP. 55–59.
The financial stability of the banking sector largely depends on effective banking regulation and supervision. The quality of preventive banking supervision depends on the quality of forecasting the financial performance of credit institutions. When choosing a financial performance forecasting model, you should take into account a number of features that are inherent in the financial sector, such as the depth of historical data and the need for expert interpretation of the results. The modeling should also take into account both factors from the internal reporting of the bank, and external – from the reporting of other banks and various macroeconomic indicators. The correct construction of the system model using artificial intelligence, its validation, as well as constant monitoring of the model's risks will allow achieving maximum results in the field of forecasting the financial situation of credit institutions.

Key words: banking supervision, analysis of the financial condition of credit institutions, intelligent decision support systems, banking sector, linear regression, forecasting.

Baranov I., Panov A., Skorobogatov I. Representation of the Organization of Complementary Display Devices of the Situation Center. – PP. 60–64.
The presentation of the organization of complementary display devices in the situational center is proposed to improve the ergonomic properties of the conference room by redistributing low-dynamic information of an organizational and informative nature to them, which ensures a decrease in the deficit of information about the surrounding space and the topics discussed.
Key words: situational center, display system, organization model.

Bashkirtsev A., Parashchuk I. Determination of the Informative Significance of Requirements for Quality Indicators of the Technical Basis of the Communication Management System. – PP. 65–69.
An approach to solving the problem of determining the volume and nomenclature of requirements for quality indicators of the technical basis of the communication management system is considered. This approach allows us to obtain estimates of the relative informativeness of requirements, and is also based on a multi-criteria ranking according to the informativeness of the initial set of requirements describing the system with resource constraints to achieve the required effectiveness of the automated communication management process.
Key words: communication, management, technical basis, requirements, system, quality indicator, informativeness, matrix, significance.

Bayagantaeva E., Musaeva T. Efficient Image Generation Tools. – PP. 69–73.
This article discusses existing products for creating paintings, their features and differences, as well as the potential for using images as a successful commercial object. These programs allow person not only to express creatively, but also to make unique images for advertisement, books covering, clothing design, etc. in a short time.
Key words: neural network, convolutional neural network, generative adversarial network, image generation.

Belov S., Makarov L. Territorial Monitoring Based on Automatic Mobile Communications. – PP. 74–77.
ZigBee technology is becoming more and more popular due to its universal network topology, which gives great flexibility in deploying a local network, as well as low power consumption of its modules and variability of operation in one range of electromagnetic waves, which in turn provides a wide range of applications, and the development of robotics provides an opportunity to combine these technologies and find their own niche.
Key word: Zigbee technology, Wi-fi, Bluetooth, automation, robots.

Belous K., Pilikina E. Training Stand for Research of Microcontroller Boards and Electronic Modules of Small Automation Systems. – PP. 78–81.
Modern small automation systems in most cases contain a microcontroller board with firmware that ensures the operation of the device according to a given algorithm, as well as sensors and

actuators. When prototyping them, one of the important issues is the issue of ensuring a reliable connection between the components of electronic circuits.
Key words: automation, printed circuit board, microcontroller, automation.

Bondarenko I., Martynov D. Process Control Mechanisms in High-Performance Platform Operating Systems. – PP. 82–87.
Study of the principles of operation of parallel computing systems for multicore processor devices. Determination of current operating systems and process control mechanisms.
Key words: process control, high performance platforms, parallel computing.

Branitskiy A., Mardanov R. Detection Voice Spoofing Based on Convolutional and Recurrent Neural Networks. – PP. 87–91.
In this work, a study of models of deep neural networks used in solving the problem of detecting falsification of voice has been carried out. To train the models, spectrograms were prepared from voice samples using the Hamming window. Models were trained on prepared spectrograms using the following architectures: only recurrent neural networks using long short-term memory (LSTM) or gated recurrent units (GRU), only convolutional neural networks Conv1D (for convolution over window spectra) or Conv2D (for convolution of the entire spectrogram) and a combination of both architectures with combinations (LSTM + Conv1D, LSTM + Conv2D, GRU + Conv1D, GRU + Conv2D). Comparison of the results of the proposed models is given, which makes it possible to evaluate the accuracy of voice falsification detection for each model (architecture).
Key words: recurrent neural networks, convolutional neural networks, machine learning.

Bunyakina E., Galchenko M., Guschinsky A. Electricity Consumption in the Context of the COVID-19 Pandemic: Case Study. – PP. 92–96.
Time series analysis and forecasting displays abrupt changes in the environment that can lead to the breakdown of time series trends. Recent events related to the COVID-19 quarantine raise a new question: to what extent do the decisions taken to isolate citizens and change the operating mode of enterprises change the patterns of electricity consumption.
The target of the work. To investigate the impact of the COVID-19 pandemic on electricity consumption using data from 50Hertz Transmission GmbH.
Key words: COVID-19 pandemic, time series, data, energy, electricity.

Vaganov A., Ivanov A. Development of a Method for Designing a Primary Signal Processing System. – PP. 97–101.
The article discusses issues related to the development of a method for designing a preprocessing path for a signal from primary measuring transducers (sensors) for use in various automated control systems. The synthesis of the structure and description of the blocks included in the preprocessing system are performed.
Key words: discrete analog circuits, synthesis, analysis, processing path, structure.

Vaganov A., Seregin S. Modern ICS Power Supply Design. – PP. 101–105.
This paper is directed towards the questions of power supply design in modern ICS production facilities. A review of existing PSUs was given along with a structure that complies with the primary requirements for them. Specifics for building a PSU with a new method were also

given. Some practical recommendations were given for building primary and secondary PS devices for ICS, connecting them into blocks and placing them inside the systems in a way that would allow for increased reliability and decreased influence of the noise on other ICS systems.
Key words: PSU, ICS, automation, power supply, power allocation.

Varlamov M., Tsibulya A. Evaluation of the Efficiency of Visualization of Integration Detection Systems. – PP. 106–111.
The article describes a methodology for assessing the effectiveness of a visualization subsystem based on the ELK Stack software package for intrusion detection system. The algorithm of functioning of the subsystem, an example of the visualization panel, based on the analysis carried out among the most popular intrusion detection system, are presented. The methodology for evaluating the effectiveness of the visualization subsystem considered in this work is aimed at increasing the operator's productivity in identifying security incidents.
Key words: intrusion detection system, visualization subsystem, performance evaluation.

Vasilchenko V., Voloshinov D. Functional Features of User Interfaces of Learning Management Systems for Different Categories of Users. – PP. 111–114.
Distance learning is the highest priority for certain categories of users, especially for people with disabilities. Along with that, the functional features of user interfaces of learning management systems in this case should have extended functionality to meet the needs of users. The article discusses the basic and sufficient functionality for comfortable learning through the LMS for different categories of users with disabilities. The use of additional functionality and modern technological capabilities for the implementation of distance learning will make education more accessible to a wide audience, and will make the learning process more comfortable.
Key words: learning management systems, e-learning resources, comfort reading panel, disabilities.

Velyugo A., Filippov F. Research of Timely Access Problems to Up-to-Date Information in Corporate Information Systems. – PP. 115–118.
The transition to the digital economy of system-forming corporations and public service bodies is inefficient without the introduction of ontological information and reference web services into the perimeter of the corporate information system. The article describes the main reasons for implementing your own solution within the perimeter of the corporate information system, and also describes the main pai-pline for converting data into a structured search results document.
Key words: cognitive search, corporate information system, data processing.

Verkhova G., Kolesov D. Research and Development of Island Models of Non-Blocking Multithreaded Genetic Optimization Algorithms for Machine Tools with Numerical Control. – PP. 119–122.
Path optimization is a common task of the present time, since the complexity of such a task increases many times with the growth of route points. To solve path optimization problems, heuristic algorithms are commonly used. An island model of non-blocking multithreaded genetic algorithms for path optimization for machine tools with numerical control is

investigated and developed, experiments are carried out and the acceleration time of the algorithm is calculated.
Key words: genetic algorithm, actuator, trajectory optimization, operators, crossing over, mutation, machine learning.

Verkhova G., Kupcov A. Algorithmic Software for Visualizing the Process of Solving Optimization Problems using Genetic Algorithms. – PP. 123–126.
Computer graphics are a modern and effective method for analyzing scientific data. In this paper, we propose an implementation of an algorithm for visualizing the functioning of a genetic algorithm in real time. The genetic algorithm is used to optimize the laser trajectory of a machine with numerical software.
Key words: visualization, optimization, genetic algorithms, programming, evolutionary computing.

Verkhova G., Prokof'ev P. Synchronous Localization and Mapping Techniques for Autonomous Vehicles. – PP. 127–129.
The results of research of methods of simultaneous localization and mapping for autonomous vehicles are presented. Comparative analysis of SLAM methods is performed. The ways of constructing libraries of software and algorithmic support for methods of localization, construction and updating of geoinformation multidimensional models are considered. It is shown that at the present time for compact unmanned ground vehicles, in most cases, methods using information obtained from the Lidar seem to be preferable. Ways of integrating heterogeneous information into an on-board computer of an unmanned vehicle using multidimensional models are considered.
Key words: scale, mapping, autonomous vehicles, SLAM, ROS.

Verkhova G., Fedorov N. Multilayer Structure of the Hardware and Software Complex for the Control of an Underwater Unmanned Vehicle. – PP. 130–134.
The multilayer structure of the hardware-software complex for the control of an autonomous underwater unmanned vehicle is presented. It is shown that the proposed multilayer structure will ensure the unification of the software, algorithmic and hardware support of autonomous underwater vehicles in the implementation of various control functions (holding the location of the underwater vehicle under conditions of constant external influence of the current, automatic control of movement along the bottom surface having a complex relief, movement of the vehicle along a given trajectory etc.). The proposed approach will provide the possibility of a flexible combination of various control algorithms for an autonomous underwater vehicle, as well as the adaptation of mathematical and software-algorithmic support for various types of robotic underwater vehicles.
Key words: unmanned underwater remote-controlled vehicles, stabilization, architecture of control systems.

Verkhova G., Shabanov A. A Model for Integrating the Academic Cyber Environment. – PP. 134–139.
The article presents the results of research on the problem of forming a unified digital ecosystem of higher education and the formation on its basis of a unified academic cyberspace.

It is shown that the formation of an ecosystem requires a single academic cyber environment, which will become its basis.
Key words: digital ecosystem, unified academic cyber environment, cyberspace, higher education.

Vishnevskiy A., Markin D. Prototype of Electronic Voting System Based on a Protocol with Separated Secret and Active Authentication Devices. – PP. 139–144.
The article provides a proposal for the implementation of a prototype of an electronic voting system based on a secret sharing protocol and active authentication devices. The main requirements for electronic voting systems are given. A structural diagram of the main components of the electronic voting system is developed. Conclusions are formulated regarding the development of this technology.
Key words: blockchain, anonymized processing of personal data, secret sharing, electronic voting.

Vladykin M., Gromov V. Raspberry Pi Linux Distribution Influence on SQLite DBMS Performance. – PP. 145–148.
An important part of software development is databases interaction implementation. At the same time, it is required to ensure the minimum delay in updating the values in the databases. Also it is necessary to provide sufficient performance when implementing a graphical user interface so that the user does not experience discomfort when using the program. The article examines the influence degree of graphical user interface presence in operating system on SQLite DBMS operation using a single-board computer of the Raspberry Pi family.
Key words: databases, database management system, graphical user interface, SQL, SQLite, Linux, Raspberry Pi.

Vladykin M., Gromov V. SQLite API Work Optimization on Raspberry Pi Microcomputer. – PP. 148–152.
An important part of software development is databases interaction implementation. At the same time, with low computational capabilities of the system, it may be necessary to implement optimizations in the program code in order to reduce the delay in the execution of SQL queries. The article demonstrates working methods for optimizing work with the SQLite DBMS API using the example of a single-board computer of the Raspberry Pi family and the C ++ programming language.
Key words: databases, database management system, API, C/C++, SQL, SQLite, Linux, Raspberry Pi.

Voloshinov D., Gencheva A. Creating user Experience based on the Learning Factor Due to Erroneous Actions. – PP. 152–155.
The article is devoted to the process of creating user experience based on the learning factor in case of erroneous actions in terms of cognitive psychology, in particular, the sequential use of different types of memory: sensory, working and long-term. The negative and positive emotional impact acts as an influencing stimulus. Limitation of brain activity is envisaged. The effectiveness of creating user experience during targeted use due to learning was determined as a result of the conducted usability testing of the administration section in laboratory subsystem of the medical information system "Ariadna".

Key words: user experience, cognitive psychology, sensory memory, working memory, long-term memory, hypothalamus.

Voloshinov D., Kravchenko A.-M. Development of an Information System Model to Support the Educational Process in the Conditions of Application of the Augmented Reality Means. – PP. 155–159.

Augmented reality technology in education is filling an educational niche increasingly and globally. E-books, interactive whiteboards, tablets-all of it helps to improve the educational process and make it more effective. The problem and purpose of the article is to study the prospects of technologies and innovative development of educational services in the field of geometry. The relevance of the problem is due to the rapid development and introduction of information and communication technologies in various areas of public activity, including the educational sphere. The article reveals the concept of augmented reality technology and examines the role of information technologies in the educational process. The author pays attention to the structure of the augmented reality application and the algorithm of its operation.

Key words: augmented reality (AR), education, technology.

Volynkin P., Kononiuk O. Investigation of the Steganographic LSB Method with Adaptive Search for Data Embedding Areas in Raster Graphics Covers. – PP. 159–163.

In most existing stegosystems, the choice of embedding regions is strictly determined by algorithms without taking into account the peculiarities of the used cover image and the size of the attached message, as a result of which the regions of a single image are "distorted", which leads to a deterioration in the perception transparency. This article proposes an adaptive approach to determining the number of least significant bits of a pixel depending on its belonging to a homogeneous area or edges of the image.

Key words: steganography, graphic files, LSB, edge detection.

Vostrukh A. Evaluating the Aesthetics of the Color Scheme of Graphical user Interfaces. – PP. 163–167.

The article deals with the problem of evaluating the aesthetics of the color scheme graphical user interfaces. Using the existing constants obtained experimentally in the disciplines of ergonomics and engineering psychology, it is planned to develop an approach capable of evaluating interfaces for the complexity of user perception of information and functional elements and the color scheme of interfaces.

Key words: GUI, evaluation parameters of the interfaces, effect of stereochromatism, color associations, color scheme.

Gorokhov A., Kosolapov V., Lipatnikov V. Model of the Database Security Management Process in the Information and Computing Network. – PP. 167–171.

In modern conditions, any activity is associated with the operation of large amounts of information, which is produced by a wide range of people. Objective: To develop a model of the database security management process in the information and computing network. Data protection from unauthorized access is one of the priority tasks in the design of any information system. As a result of the recently increased importance of information, there are high requirements for data confidentiality. Results: The determination of the values of the

characteristics of a security breach that are important for making a decision to respond to an identified computer incident is carried out using a cognitive map. Database management systems, especially relational databases, have become the dominant tool in this field. The novelty lies in the use of a cognitive map to ensure the security of databases. Practical significance: the developed model allowed us to determine further scenarios for the development of information security of the database. Ensuring the information security of the DBMS becomes crucial when choosing a specific means of ensuring the necessary level of security of the organization as a whole.
Key words: information security, information security of database management systems, database security management process, cognitive map model.

Gorshenina A., Musaeva T. Comparative Analysis of Mobile Applications for Electronic Publications Reading. – PP. 172–176.
A modern person receives most of the information through the screen of a mobile phone, constantly from different sources. The media are fighting in this stream for the attention of readers, and commercial print publishers have to adapt to a new electronic format in order to maintain and grow their audience. The article analyzes mobile applications that are a platform for placing one or several digital publications. The aim of the article is to identify common functional and interface solutions, evaluate and compare them. Comparative analysis affects the patterns of information presentation, navigation features, differences between the digital and the printed format, and usability. The research results can be used by publications when adapting in the digital environment, as well as become the basis for new patterns of content placement and interaction with it.
Key words: media, magazine, mobile applications.

Grishin N., Kosov N., Mazepin P. Relevance of Methods to Combat DDOS Attacks. – PP. 176–179.
The aim of the study is to analyze the relevance of methods for combating DDOS attacks, which are currently one of the most popular methods of attacks aimed at a computer system in order to bring it to failure. The article discusses the most popular and at the same time effective methods of countering this type of attacks. The cost of implementing each of the methods and their areas of application will be considered separately. Also, the main pros and cons of each of the methods will be considered and ways of developing certain methods in order to increase their effectiveness are presented. As a result, the optimal control method will be selected based on the cost of implementation and efficiency.
Key words: DDOS, DOS, information security.

Gromov V. Kompass 3D-LT Version 12 as an Undervalued Tool for Modern Engineering Graphics. – PP. 180–186.
The report examines the methodology for teaching students using computer-aided design systems (hereinafter – CAD) Compass-3D versions 12–19 when performing educational tasks in the discipline "Engineering and Computer Graphics" at the St. Petersburg State University of Telecommunications. prof. M. A. Bonch-Bruevich. The given methodology is based on many years of experience in teaching students in the period from 2013 to 2021.
Key words: interstate standards, national standards.

Gromov V. Prospects for the Development of Computers Based on ARM Processors. – PP. 186–190.
The report discusses the main directions of development of microcomputer systems in the educational process. Examples of creating information systems in the educational process based on ARM processors are considered. The article deals with the issue of teaching the skills of administration of complex information systems on the example of using platforms based on an ARM processor.
The possibility of using modern academic programs in the educational process on the use of modern operating systems with the ability to build models simulating complex industrial systems is discussed.
Key words: microcomputers, information systems.

Gromov V., Skorobogatov K. Defining the Procedure for the Functioning of the Developed Software for the Storage and Exchange of Electronic Departmental Research Materials in Multi-user Mode. – PP. 190–194.
The article is devoted to determining the operating system for server software based on the chosen technology stack: Python programming language and MariaDB database management system. It contains the results of synthetic server testing and comparative analysis of the most popular modern server operating systems based on the Linux kernel. Practical application of the results of the study will allow you to competently choose a server operating system in accordance with the specified tasks.
Key words: ubuntu, Debian, CentOS, server OS, synthetic testing.

Gubin A., Litvinov V., Filippov F. Research of Information Efficiency of Digital Smoothing Filters. – PP. 195–197.
Currently, the use of information estimates in the tasks of intellectual analysis of the occurrence of states of uncertainty in data processing systems of various nature is quite relevant. In this paper, we consider methods for evaluating the influence of digital smoothing filters on their information efficiency when smoothing additive random noise and isolating the useful component of the input signal. The research is based on the analysis of changes in the entropy and dynamics of information processes of smoothing random signals.
Key words: information, intelligent analysis, filtering, Kolmogorov complexity.

Gubin A., Litvinov V., Filippov F. Application of Neural Network Technologies in Information Systems Decision Support. – PP. 198–203.
Maintenance and support of information systems is carried out by technical support services. With the expansion of the supported infrastructure, the workload on the support team increases, the number of specialists increases, and special methodologies and tools for support management are applied. At present, of the greatest interest are intelligent decision support systems that assist decision-makers in making these decisions using neural network tools. The paper proposes modern approaches based on natural language processing (NLP).
Key words: intelligent decision support systems, natural language word processing, NLP.

Gubin A., Litvinov V., Filippov F. Variation Pooling Procedures for Modeling Retina. – PP. 203–208.
Procedures for modeling lateral connections in the plexus-like layers are proposed. The model is based on the principle of using non-uniform subsampling. The research is based on the analysis of the functioning of horizontal and amacrine cells of the retina from the point of view of machine modeling. The proposed models can find their application in new neural network architectures.
Key words: computer vision, retina, neural networks, pooling.

Gunina E., Ivanova S. Method for Visualization of Results UX-testing Information Resource. – PP. 208–213.
The article analyzes the eye-tracking and mouse-tracking usability testing technologies and methods for visualizing the results of UX testing of an information resource. A study is presented that allows to reveal the relationship between tracking the trajectory of the user's eye movement, the movement of the mouse cursor and the clicks made by the user. The relevance of this research lies in the fact that the methods of visualization of UX testing allow us to qualitatively analyze the appearance of the Internet page and navigation on them in order to improve usability, and there is a need to consider these methods in more detail with a view to further practical application. The possibility of creating a new method for visualizing the results of usability testing is considered.
Key words: mouse-tracking, eye-tracking, UX-testing, results visualization, usability.

Gunina E., Rozhdestvenskiy D. Analysis of Tools for Creating Interactive Elements of a Musical Application for Learning to Play Various Instruments. – PP. 214–218.
The article examines the means of creating interactive elements of an application for learning to play on various instruments. A brief description of the creation and operation of interactive elements in various programs is given. In the course of studying the material, a comparative analysis of development tools and methods is carried out, the positive and negative aspects of these developments are revealed. As a result of researching modern sources of information, we can single out several of the most popular, as well as frequently used tools for developing interactive elements.
Key words: application, virtual reality, interactive element.

Dagaev A., Kovalenko L. Generation and Search for Shortest Path in Two-Dimensional Labyrinths. – PP. 218–224.
Algorithms for generating and finding the shortest path in two-dimensional mazes, as well as their characteristics are considered. The aim of the study is to determine the dependence of the running time of the algorithms for finding the shortest path on the characteristics of the labyrinths. All considered characteristics are described in detail. Such generation algorithms are selected, the resulting labyrinths of which have different characteristics, which makes it possible to determine the desired dependence. The mazes are generated by the following algorithms: Aldous — Broder, Recursive Backtracking, Growing Tree, Sidewinder, Rooms and Vertical Blocks. The following algorithms perform the shortest path search: "A" with four heuristics and "BFS" (Breadth First Search). The peculiarity of the application of the result of this study lies in the fact that the fastest search algorithm can be selected for the generation algorithm or for the specific characteristics of the already generated maze.*
Key words: generation of ideal and non-ideal mazes; search for the shortest path, optimization.

Dagaev A., Chmelev M. Comparative Analysis of Different Models of Neural Networks and Loss Functions in the Problem of Segmentation of Skin Diseases. – PP. 224–229.
Recently, the problem of segmentation in medicine has become more and more urgent. This article discusses the problem of skin disease segmentation using various machine learning models. The article provides a comparative analysis of the result of training convolutional neural network models using various loss functions. The results of the operation of the models on the validation set are presented.
Key words: SegNet, U-net, Dilated U-net, convolutional neural network, Focal loss, Tversky loss, Dice loss, segmentation.

Eremenko A., Kokorev A., Slesarchik K., Shvedov S. Problems of Implementation of Modern Systems for Detecting Cyber Attacks. – PP. 230–234.
The article deals with the conceptual difficulties of implementing systems for detecting cybernetic attacks on a modern electronic database using statistical and heuristic methods for detecting destructive information cybernetic influences. The directions of overcoming the problems mentioned in the article are proposed, which allow us to bring the existing imbalance in the characteristics of infocommunication networks and the capabilities of cyber attack detection systems into line.
Key words: cybernetic attack detection system, multi-vector DDoS-attack, artificial neural network, infocommunication network, destructive cybernetic information impact.

Zharanova A., Ptitsyna L. Computational Intelligence used in Information Security Monitoring in Distributed Accounting Systems. – PP. 235–239.
With regard to modern approaches to the creation of artificial intelligence systems, the key directions of the development of computational intelligence are highlighted. The article considers methods of introducing computational intelligence into monitoring of information security of distributed accounting systems. The special mathematical aspects that concern the information security means integration while ensuring information security of distributed accounting systems are described. Methods for the formation of computational intelligence used in information security monitoring in distributed accounting systems in function of the concurrent threat detection are disclosed.
Key words: computational intelligence, information security, complex information security systems, monitoring, distributed systems.

Ivanov S., Smirnov I., Fedorov P. Calculation of a Fiber-Optic Power Divider Based on Phase-Contour Equivalent Circuits. – PP. 240–245.
This paper considers the application of a new analytical approach based on the theory of synthesis of optical heterostructures, to the calculation of fiber-optic power divider, which will make it possible to obtain a product with improved technical characteristics. The analysis of the technologies used today for the manufacture of power dividers is given.
Key words: passive optical networks, optical power divider, optical filter, multiplexer, optical splitter.

Izrailov K., Pokusov V. Creation of a Software Object-Oriented Platform for the Development of UEFI Modules. – PP. 246–250.
The paper deals with the task of developing modules using UEFI. Some problematic issues that arise in this case are indicated, such as insufficient functionality of the C language used, the complexity of logging operations, as well as the impossibility of direct debugging of the code. As an alternative approach, a developed platform is proposed and described, which makes it possible to more conveniently develop modules. Its advantages include such as the use of the C ++ programming language and a large set of wrapper classes over UEFI functionality, the ability to log actions, a built-in C interpreter for debugging in pseudo-interactive mode, the presence of primitives for creating textual graphical interfaces with a set of windows and their standard elements as well as support for streaming cooperative multitasking. The development of the platform is completely original.
Key words: BIOS, UEFI, module, development, platform, advantages and disadvantages.

Ilina O., Kupchinenko O., Skoropad A. To the Question about Changes in the System of Information's Security in Operating Systems of Special Purpose. – PP. 251–254.
The analysis of the differences in the system of information's security in operating systems of special purpose Astra Linux SE Smolensk, version 1.6 was done. The mandatory entity-role model of access control and information flows which contains additional ways to differentiate access, were explored. The features of the application of the mandatory integrity control regime are analyzed.
Key words: operating system of a special purpose, information security, mandatory model of access control, mandatory integrity control, privileges.

Ilina O., Kupchinenko O., Skoropad A. About Protected Complex of Email Programs from Modern Operating Systems of Special Purpose. – PP. 255–258.
The analysis of the protected complex of email programs from operating system of a special purpose Astra Linux SE was done. Mechanisms for increasing the security of mail correspondence were explored. The questions of application of encryption software and digital signature creation in mail messages were analyzed.
Key words: operating system of a special purpose, email, mail server, mail client, public key, private key. digital signature.

Ilina O., Kupchinenko O., Skoropad A. Access Control in DBMS in Operating System of a Special Purpose. – PP. 259–263.
The aspects of database administration in operating system of a special purpose «Astra Linux SE» are analyzed. The analysis of access control mechanisms implemented in the DBMS PostgreSQL in operating system of a special purpose Astra Linux SE is carried out. The tools for mandatory credential and discretionary rights of access control in the PostgreSQL are considered.
Key words: operating system of a special purpose, database management system, mandatory model of differentiation of access, discretionary model of differentiation of access.

Ilina O., Kupchinenko O., Skoropad A. Network Authentication Service. – PP. 263–268.
The analysis of the features of the network authentication protocol Kerberos, which is focused on the client-server model and provides a high level of information security. The terminology

and operating principle of the Kerberos protocol, which allows data to be transmitted over unsecured networks for secure user identification and provides mutual authentication, are considered. The aspects of Kerberos administration in the special-purpose operating system "Astra Linux SE" are analyzed.
Key words: authentication, network authentication service, operating system, Kerberos protocol, client-server model, ticket, key distribution center, realm, domain, principal.

Kozin S., Markin D. The Complex of Algorithms for Determining the Location of Mobile Sources of Radio Signals Based on Forecasting Methods. – PP. 268–274.
The article presents the main research results, such as the implementation of a complex of modeling algorithms that carry out a number of random processes: the movement of mobile sources of radio signals and the propagation of radio waves; algorithms that implement the analytical calculation of the estimated location area based on the fuzzy logic apparatus, as well as the forecasting method (linear prediction). A number of experiments, including full-scale ones, were carried out, allowing to use as initial data the real distribution of statistics of the received power level of the cellular network of the LTE standard, as well as experiments aimed at studying the effectiveness of the mathematical apparatus of fuzzy logic in con-junction with forecasting. Conclusions are formulated regarding the results of the studies.
Key words: positioning systems, wireless data networks, trilateration, fuzzy logic.

Koloskov N., Fedorova A. The Process of Creating a 3D Character and Ways to Automate its Stages. – PP. 274–277.
The article is devoted to the process of creating a 3D character for further use in game development. A description of the pipeline for developing a 3D model is given. With the help of illustrations, some stages of development are clearly shown. Examples of stages automation, their advantages and disadvantages are given. Based on the review given in the article, conclusions are drawn about the current state of affairs in the area under consideration and the prospects for its development.
Key words: 3D, game models, sculpting, retopology.

Koltsov P., Musaeva T. The Method of "Quick Commands" as a New Experience of Listening to Musical Compositions. – PP. 278–280.
This article describes the role of quick commands in a process such as listening to music. Potential innovations that could improve our music listening experience are sometimes overlooked. Users interact with the audio player using a standard set of buttons – listen, pause, rewind, fast forward, etc. This does not mean that this interaction experience has reached perfection. This article discusses the concept of quick commands and how they can be used to improve the audio player experience.
Key words: quick commands, listening experience, audio player, user interface, information systems.

Krivonosova N., Tereshchenko N. Development of an Information System for Accounting of Equipment at the Enterprise. – PP. 281–284.
Accounting of equipment at the enterprise is one of the compulsory business processes. The existing software solutions for automation of equipment accounting today are not always

available at the cost of purchase and operation, and also do not always fully meet the requirements of the company.
Key words: information system, equipment accounting.

Kryukova E., Parashchuk I. Substantiation of the Stages of the Method of Interval Estimation of the Quality of Electronic Libraries. – PP. 285–289.
The article deals with the analysis of the essence and content of the stages of the method of interval assessment of the quality of functioning of modern electronic libraries. The sequence of implementation of these stages, their functions and tasks are analyzed. The study was conducted to systematize and identify the features of determining interval (lower and upper) quality ratings of electronic libraries based on the methods of the theory of interval averages in the interests of reliable analysis and improving the quality of management of the structure, parameters and modes of operation of systems of this class.
Key words: electronic library, indicator, quality, interval averages, estimation, method, stages.

Lepeshkin O., Manukov K., Ostroumov M., Ostroumov O., Titov S. Objects Ranking of Critical Information Infrastructure of the Communication System. – PP. 289–295.
One of the properties of communication is safety, the communication system PROPERTY is stability, while the communication system DEPLOYMENT in any conditions of exposure to destabilizing factors must ensure its stable and safe functioning. The Federal Law of 26.07.2017 N 187-FL "On the security of the critical information infrastructure (CII) of the Russian Federation", adopted in 2017, introduces the criticality CONCEPT of the information infrastructure and its facilities. One of the stages of determining the critical information infrastructure objects LIST is the process of assigning them a category of importance. To determine which of the objects of the critical information infrastructure SUBJECT is the most important, a ranking procedure can be carried out in order of importance. The paper presents some approaches to ranking objects by importance.
Key words: critical information infrastructure, critical facility, information security, control system.

Litvinov V., Novikov E. On Neural Networks' Usage for Pattern Recognition Problem Solving. – PP. 295–299.
Usability of neural networks for solving pattern recognition problem is being examined. The mismatch between theoretical problem definition and practical solving algorithms is shown. Also the experiment for showing neural network performance on solving pattern recognition problem is run. As a result, statement about low usability of neural networks for solving pattern recognition problem is proposed.
Key words: pattern recognition, regression, statistical learning theory, empirical risk minimization, machine learning, neural networks, multilayer perceptron, gradient descent.

Litvinov V., Novikov E. Neural Network Pruning with OBS and L-OBS Algorithms. – PP. 300–304.
Usage of neural network pruning is being examined. Only feed-forward neural networks are used in this paper.

Algorithms Optimal Brain Surgeon (OBS) and Layer-wise Optimal Brain Surgeon (L-OBS) are being compared. Specifically, author is interested in impact of pruning on loss value of neural network. It is demonstrated that L-OBS algorithm shows better results than OBS algorithm. In addition author is examining pruning impact on neural networks' VC-dimension (it's higher bound).
Key words: machine learning, neural network, multilayer perceptron, neural network pruning, OBS, Optimal Brain Surgeon, VC-dimension.

Litvinov V., Radnaeva I. The Analysis of Methods for Recognition the Aggressive Behavior on Video Images. – PP. 305–310.
While the problem of actions recognizing has become a frequently discussed topic in computer vision, the identification of aggressive behavior has been generally less studied. Automated recognition of this type of human behavior will have a great effect in some video surveillance scenarios, for instance, in prisons, schools, psychiatric centers or other similar institutions. The article is devoted to some methods of computer vision that allow identifying the aggressive human behavior to notify the relevant emergency services and prevent the negative consequences of aggressive behavior.
Key words: aggressive behavior, computer vision, face recognition, convolutional neural networks.

Litvinov V., Ruigo D. Automation of Lithological-Facial Analysis Methods through the Application of Machine Learning Technologies. – PP. 310–313.
This paper is aimed at analyzing the methods of lithological-facies analysis of oil and gas bearing strata for their automation through the using of modern machine learning technologies. In this work, the existing achievements of specialists in geological and computer sciences in the field of using intelligent methods of processing geological data at various stages of lithological-facies analysis of oil and gas bearing strata are studied, actual problem situations and tasks for the implementation of machine learning tools are identified.
Key words: lithological-facies analysis, geological exploration, machine learning, classification, neural networks.

Markin D., Minachev V. The Malware Recognition Algorithm for ARM Architecture Processors Based on Dynamic Analysis and Detection of Suspicious Features. – PP. 314–319.
The article provides an algorithm for analyzing the program execution traces for ARM processors. A model of malicious software has been built. A scheme for classifying a program as malicious and a method for detecting suspicious behavior were developed. The effectiveness of the method was assessed using the developed prototype of the software.
Key words: dynamic analysis, exploit, shellcode, assembly code, polymorphic code.

Markin D., Nikiforova E. Application of HASP Technology for Protecting the Information System from Unauthorized Use. – PP. 319–324.
The paper describes the technology of protection against unauthorized use of an information system, access to the resources of which is carried out remotely, based on the use of HASP technology, hardware identifiers - tokens, and the technology of intercepting system calls using the LD_PRELOAD parameter.
Key words: information system, HASP, interception of system calls, copyright protection.

Markin D., Rykov D. Analysis of Methods for Deobfuscation of Source Codes of Web Applications in JavaScript. – PP. 324–329.
In this article contains a study and analyze static methods for deobfuscating transformations of program code in JavaScript. Describes the main methods of protection against the analysis of program code in JavaScript. The method of obfuscation of JavaScript code as the main means of protection against analysis was investigated.
Key words: JavaScript, obfuscation, deobfuscation, code emulator, web application.

Markin D., Schukin A. Automating the Creation of a Distributed Network Node Based on Selenium WebDriver Technology. – PP. 329–334.
The article describes the principles of building distributed computing networks, an analysis of their advantages. An example of the implementation of the automated process of creating a distributed computing network node using the Selenium WebDriver web application testing tool and the python high-level programming language is analyzed.
Key words: distributed computing network, Selenium, Selenium WebDriver, python, P2P.

Maslakov M. Analysis of the State and Prospective Directions for Development of HF Data Modems. – PP. 334–338.
The paper presents an analysis of existing data modems in the HF channel. Some urgent problems for long-distance HF communication are highlighted. The directions of development and improvement of models, signal-code structures and algorithms for their processing are shown to increase the probabilistic-temporal indicators of the radio link.
Key words: data modem, HF channel, adaptive communication.

Makhortov S., Puzanov I., Fedorova A. Consideration of the Conceptual Principles of the Use of Animation When Designing a User Interface. – PP. 338–341.
The use of animation is currently a trend in the development of interfaces for various software products. Many interface design tools offer a wide range of options for implementing these functions. But the need to use animation special effects in the interfaces of software products leads to additional time and financial costs that are not due to the practical benefits for the functioning of the software. The article discusses the types of animation used in programs, analyzes the problems arising from the excessive use of animation and the resulting consequences. Appropriate conclusions are drawn.
Key words: animation, functional animation, emotional animation, user interface design.

Metelkov A. On the Method of Differentiation of Confidential Information in Information Processes in the Interaction of GIS. – PP. 342–345.
The success of emergency response managers in developing management decisions depends on their awareness, based on the interaction of information systems. The effectiveness of the interaction of information systems is determined by the organization of data exchange, commands and signals, which provides for the differentiation of confidential information in information processes.
Key words: confidentiality, information, information processes, information exchange, differentiation.

Mikhaylichenko A., Mikhaylichenko N., Parashchuk I. Formulation of Stages and Features of the Development of a Methodology for Assessing the Reliability of Modern Mobile Data Centers. – PP. 345–349.

The analysis of scientific and practical approaches to improving the methodology and tools for assessing the reliability of modern mobile data centers is carried out. The main content of the article is formulation of goals and detailed description of the stages of development of a technique of multi-criteria estimating the reliability of mobile data centers in different conditions, taking into account various aspects of uncertainty of the input data, which can be considered in the context of mathematics of granular calculations.

Key words: mobile data center, assessing, data processing, reliability, methodology, system, indicator, fault tolerance, stage.

Michal G., Tarasov V. Development of an Information System for Managing the Life Cycle of Electronic Products. – PP. 349–354.

Today, due to the great competition, enterprises that produce electronic equipment are forced to find new ways to optimally organize their work. This business, like any other, is aimed at profitable work and the fulfillment of all customer requirements in the allotted time. Many processes in the design of printed circuit boards need automation. Large enterprises have funds for expensive software, and they usually have programmers and system administrators who have the appropriate competence to work with such software, but small organizations do not have the funds for this. Paper document flow, which generates a lot of errors, non-centralized storage of files, libraries, documentation, lead to large delays in production, which can lead to huge losses. Using new technologies, the company systematizes and automates the work, thereby saving labor and material resources.

Key words: information system, electronic products, life cycle, electronic components, use case diagram.

Mogush L., Smorodin G. Technological Convergence in Digital Economics. – PP. 355–358.

Usage of expert system in higher education including student knowledge testing systems was analyzed. Restraining factors were clarified. The concept of individual self-education trajectory was introduced.

Key words: digital economics, technological indicators, convergence clubs, digital technological convergence.

Musaeva T., Ukrainets Yu. Features of Designing a Web Interface for Visually Impaired Users. – PP. 359–362.

In the life of every person, digital technologies play a rather significant role, the speed of development of which is becoming more and more every year. People are willing to take advantage of the opportunities provided by the IT sector. Thanks to innovative technologies of the IT sphere, a person can easily solve not only work, but also everyday tasks, but the question arises: can everyone equally use the opportunities that this market provides us? Unfortunately, not all users interact with digital products in the same way, and very often, when developing it, we forget about people whose capabilities may be limited. Thus, based on statistics and in-depth studies of modern methods of designing the user interface for people with visual disabilities, the report will present an analysis, systematization of the data obtained and solutions to the current problem.

Key words: design system, disabilities, web technologies, assistive technologies, web accessibility.

Olimpiev A. Lifecycle Management Features of Software with Metacontrol of Functionality. – PP. 363–367.
The article describes the actual problems of creating and maintaining complex software systems, which are caused by the intensive dynamics of information technology development. The features of software products built using various ways of organizing customer-contractor interaction are considered. Possible ways to solve the identified problems set related to the organisation of the life cyrcle management of software products that are part of complex automated systems are defined.
Key words: project management, software life cyrcle, complex software systems build methods.

Orlov D., Yakovlev V. Key Sharing for the Security of the Secret Electronic Voting System. – PP. 367–372.
An electronic voting system based on a homomorphic Paillier cryptographic system is being considered. Proposals for secret sharing (decryption key) are presented, a rational number of shares is determined and participants in the electoral process to whom these shares are provided before the start of voting are determined. A procedure is proposed to restore the private key by participants before the start of the vote count.
Key words: electronic voting system, secret sharing, Paillier public-key cryptosystems, Pedersen verifiable secret sharing

Pavlovich A., Prisyazhnyuk A. Research Processes Functional Stability of Special Telecommunication Systems under Conditions Uncertainties. – PP. 372–377.
The well-known results of the study of special telecommunication systems (STS) and the influence of uncertainties on mathematical methods for assessing their functional stability are considered, as well as the choice of an option for constructing an STS based on experiment.
Key words: telecommunication systems, modeling, functional stability, destructive influences, efficiency.

Petrov G. General Analysis of Recommendations for Configuring the Security System of the Kubernetes Cluster. – PP. 378–383.
This article provides the necessary recommendations related to the security of the Kubernetes cluster. The main components of the Kubernetes cluster are considered. A number of steps have been identified to ensure the highest level of security for Kubernetes Orchestrator modules. Highlighted the sublevels of configuring Kubernetes security services. Conclusions are formulated regarding the construction of information systems based on the Kubernetes cluster.
Key words: Kubernetes, containers, DevOps, devsecops, overview, security.

Pletnev Ya., Shestakov A. Methodologies for Combined Testing of Priority Vehicle Communications using a Computer Simulation System. – PP. 384–389.
The article investigates the ways to reduce the costs of test organization of complex system-technical solutions by the example of multilayer communications of priority vehicles by means

of combined tests. It also substantiates the methodological apparatus of multipurpose application of methods and ways of analytical and simulation modeling on the basis of OMNET++, Veins, Plexe, SUMO tools for theoretical, experimental research and testing of complex system-technical solutions. The required reliability level of obtained assessments of characteristics of system-technical solutions essential properties under various test conditions is taken as a criterial basis in the research.
Key words: priority vehicles, mathematical modeling, test program, combined test methods.

Pogadaeva O., Shiyan A. A role of SEO and site design in search promotion. – PP. 390–394.
Search engine optimization methods of web resources play an important role in getting a site to the top of search queries. The article conducts a comparative study of the sites of St. Petersburg State University, St. Petersburg State University, St. Petersburg State University of Technology and a survey of 150 respondents (50 from each university). The most important factors that affect the positioning of a web page in the search results are considered.
Key words: SEO promotion, web design, website, online clients, visual communication.

Popova V., Chechulin A. Initial Events Analysis for the Safety of Nuclear Fuel Transfer Operations. – PP. 395–399.
This paper presents the formalized approach to identification and systematization of events that can lead to safety accidents. This approach allows one to form a list of necessary and sufficient protection measures against accidents, as well as to determine the redundancy in protective measures and identify accidents for which protection measures are not provided.
Key words: safety analysis methods, HAZOP method, nuclear, transfer operations, high power channel-type reactors (RBMK).

Salman W. Analysis of the Voting System in the Republic of Iraq and the Transition to an Electronic Voting system. – PP. 400–404.
The article analyzes the voting system in the Republic of Iraq and examines the main problems associated with its operation. The analysis showed that the existing voting system has security problems and needs to be upgraded with the use of information and communication technologies in order to meet international standards. It is concluded that it is necessary to use online voting in the Iraqi elections, which provides a new system of trust and security for the user and the government of Iraq. An additional advantage of such a system is the ability of voters to vote anytime, anywhere via the Internet.
Key words: voting system, voting system in the Republic of Iraq, electronic voting, online voting.

Sergiyenko S., Fedorova A. A Method for Solving the Problem of Computer Vision to Search Simple Forms in the Image Using the Hafa Algorithm. – PP. 404–408.
The article is devoted to a method for solving computer vision problems for finding simple geometric shapes in images. The principles of the Hough transformation for finding straight lines and circles are considered. The implementation of this algorithm is shown by writing code in the Python programming language using the OpenCV computer vision algorithm library. The influence of the parameters of the Hough operator on the detection of the desired shapes is shown. The possibilities of using this algorithm for solving the problem of detecting objects

are demonstrated, since simple geometric shapes are the most common forms found in the environment.
Key words: computer vision, Hough transform, OpenCV library, geometric shapes search.

Sinyk A., Tarasov A. The Evaluation of Conditions for Open Network Multi-Key Agreement. – PP. 409–413.
One of the main conditions for the functioning of telecommunications systems that use encryption methods of information protection is the secure installation of keys to correspondents. A less expensive alternative to transmission the keys over secure communication channels are the methods of key agreement in open channels. This article updates research of the formation of increased cryptocommunication of network correspondents by evaluating the conditions for the implementation of the proposed method of open network multi-key agreement.
Key words: key, information speed, open network multi-key agreement

Tarasov V. The Concept of a Mobile Laboratory Complex for the Formation of Competencies in the Field of Information Technology. – PP. 413–418.
New technological solutions in the field of electronics and computer technology open up additional opportunities for the implementation of the educational process. The problems related to the peculiarities of the laboratory and technical base used for the study of information technologies are considered. A brief overview of the hardware platforms is provided. The variants of their use are given. A variant of the laboratory complex is proposed, its advantages are reflected.
Key words: Raspberry Pi, single-board computer, educational process, laboratory complex, information technology.

Tarasov V., Chernobrovkin E. Information System for the Development of Cognitive Abilities. – PP. 418–422.
The development of cognitive functions of the brain occurs, for the most part, in childhood. The need for further development can manifest itself much later – for example, in school in the form of poor performance (difficult memorization, inability to concentrate, high fatigue). It seems logical to devote more time to problematic fragments of activity, but this approach rarely finds a response, since it is time-consuming and unattractive. To date, there are many software services that offer various kinds of improvement of the brain as a whole. It can be all kinds of puzzles or memory simulators. The issues of the effectiveness of the use of information technologies for the development of cognitive abilities are considered.
Key words: cognitive abilities, logical thinking, learning method, development systems, educational information technologies.

Tatarnikova I. Concerns About Scientometric Indicators: Causal Analysis. – PP. 422–427.
This research addresses problems related to collecting error free data characterising scientists's publication activity and quality of scientific research. The influence of scientific research on a specific area of knowledge and on science as a whole is indicated by the impact factor. This and other indicators were developed by specialists in scientometrics. There conducted a casual analysis of issues related to study, evaluation of the quality of scientific research and distortion of some date due to usage of incorrect criteria. The paper underlines

the need for critical re-evaluation of certain aspects of formation and application of indexation system for journals and ratings for assessing scientific efficiency.
Key words: scientometrics, impact factor, h-index, publication activities, citation.

Tsibulya A., Fadeev V. Malware Classification Using Recurrent Neural Networks. – PP. 428–432.
The article describes a possibility of using recurrent neural networks of LSTM architecture for malware classification. The network structure is described and the block diagram of the LSTM network module is presented. The aim of the work is to increase the efficiency of computer-technical expertise and malware analysis.
Key words: information security, malware classification, neural networks

Frolova K., Shestakov A. Mathematical Models of Risks and Structural Risk-Parameters of Infrastructure Projects. – PP. 432–437.
The article considers the problem of risk reduction in the organization of complex projects and their management based on the results of monitoring the structural risk-parameters of multiscenario systems. It also substantiates the mathematical apparatus of the formal description of risk management procedures for infrastructure projects on the example of interconnected complex systems of telecommunications and transport regional infrastructure. The authors have analyzed the traditional ways of constructing models of the complexity of systems represented in the form of a graph, ways of distinguishing the location of graphs. The authors also propose proactive procedures for managing complex projects based on monitoring the structural risk-parameters of multiscenario systems.
Key words: mathematical models of risks, complex project, graph models of systems.

Khoroshenko V. The Main Sources of the Information Security Terminology. – PP. 437–443.
This article examines the main sources of the information security terminology. Attention is focused on the information security term chosen as a system-forming term. The topic of the reasons caused the current state of terminology is considered. The relevance of the problem is highlighted and conclusions are drawn regarding the direction of development.
Key words: information security, cyber security, term, standard

Chernomyrdin V., Shiyan A. Analysis of Feedback Platforms Between Citizens and Authorities Within the Framework of the National Digital Economy Project. – PP. 443–447.
The issue of feedback between the authorities and ordinary citizens has always been quite acute. In addition to the obvious things in the form of letters describing problems from citizens, new ways and methods of communication are constantly being introduced. One of these projects is the Digital Economy, which has implemented a number of tools designed to help the authorities collect feedback from citizens, thus drawing attention to the really important issues. At the same time, feedback is collected not only on problems, but also on suggestions, albeit with slightly different tools.
Key words: state, citizens, feedback, platforms, development.

Shestakov A. Research Methodology of Licensing of Internet Services for the Transmission of Voice Information to the Public Telephone Network. – PP. 447–451.
The problems of providing and organizing the transmission of voice information to the public telephone network through Internet services are considered. The existing approaches to resolving the problems of the regulator, telecom operators and users in the legal and technical sphere are analyzed, taking into account various influencing factors, conditions and contradictions. Methodological and methodological approaches to the research of licensing of Internet services for transmitting voice information to the public telephone network are proposed.
Key words: voice transmission, internet services, telephone network.

Yaroshenko A. Formation of Requirements for Organizations to Counter Attacks on Information Resources using Social Engineering Methods. – PP. 452–456.
The paper discusses the problem of counteracting social attacks aimed at information resources of an organization. In this case, the attacked object is an employee of the organization, and the attacker is an intruder, often indirectly through software and hardware. For this, the 4 most common scenarios of such attacks are considered: a call from a bank, a fake mail letter, a "forgotten" infected data carrier and psycho-emotional impact on a person. Based on the scenarios, various approaches are proposed to counter attacks aimed at the elements of the latter: the legal user, the intruder, and the impact itself. As a result, nine generalized requirements for organizations are formed (3 for each element of the attack) aimed at countering social attacks.
Key words: information security, information resource, social attack, counteraction, requirements for the organization.

THEORETICAL FOUNDATIONS OF RADIO ELECTRONICS AND COMMUNICATION SYSTEMS

Bocharov E., Konovalova E., Sedyshev E. Microwave Generator on the Hemisphere. – PP. 457–461.
In this work, the possibility of generating a signal when placing an active bipolar in a resonator was investigated, a hemisphere is used as a volume resonator. For a detailed study of this construct, a wire equivalent of a hemisphere was created. The elements of the generator and the experimental installation of the generator on an active two-pole are developed and described. The presence of generation is investigated depending on the location of the two-pole installation and the place of energy removal. The efficiency of the proposed model is proved.
Key words: microwave, microwave generator, spherical resonator.

Bocharov E., Podolskaya M., Sedyshev E. Microwave Amplifier on Hybrid with Active Bipoles. – PP. 461–465.
The work is devoted to the synthesis of a low-noise microwave amplifier. The subject of our study is a hybrid bridge on a microstrip line and active bipoles included in its shoulders. Microwave amplifier is created on the basis of hybrid ring of adder. During the work, a layout

of the device was created on active bipoles included in the hybrid ring bridge using loops. Computer emulation of device operability and experimental studies were carried out.
Key words: very high frequency, directional coupler, ring adder, microstrip line, amplifier, amplifying diode.

Brusin E., Elgin P., Korshunov M. Measurement Receiver Preselector Design. – PP. 465–470.
The measuring receivers for measuring the parameters of industrial radio interference design becomes necessary to develop schemes for preliminary frequency selection of signals. In particular, to create circuits in the frequency range from 1 to 18 GHz. The main problem when creating a preselector is the development of amplifying circuits designed to compensate for the losses of filters and switches included in the path. The construction of a preselector using low-noise amplifier (LNA) circuits based on ultra-high-frequency (microwave) gallium arsenide field-effect transistors is considered.
Key words: electromagnetic compatibility, measuring receiver bands, microwave gallium arsenide field-effect transistor, low-noise amplifier.

Velikoborets G., Yurova V. The Major Aspects of Development of a Control System of the Anthropomorphic Robotic Arm by Processing and Transmitting of the Electrical Signals from the Brain. – PP. 471–476.
In medical technology, the development of anthropomorphic prosthetic limbs for patient habilitation is of particular interest. To facilitate the work with the prosthesis and control it, it is important to design a control interface based on the transmission of signals by electromagnetic or electromechanical means. The paper considers the main directions in the development of such interfaces, presents the results of the development of the interface and technical controls of the robotic anthropomorphic hand, which was developed at the previous stage of work and can be used as a medical prosthesis of a lost limb or as part of an automated system that simulates the work of a human hand.
Key words: semiconductor, medical electronics, semiconductor electronics, anthropomorphic prosthesis, robotics, automation.

Glukhov N., Lepikhin K., Sedyshev E. Broadband Excitation of a Circular Waveguide with a Spiral Structure. – PP. 476–482.
The work is devoted to the topic of broadband excitation of a circular waveguide. The main task of the study is to evidence of the possibility of excitation of the main electrodynamic modes of a circular waveguide in a wide frequency range. As power supply elements of the waveguide are considered spiral structures, the form of emitters of which is present as a circular, square and triangular inductances. Presents a results of the electrodynamic modeling for a number models, as well as experimental results.
Key words: broadband excitation of a circular waveguide, spiral antennas, microwave.

Kazakevich E., Odnokurtsev K., Trepalin P. Analysis of the Operation of a Parallel-Type Analog-Digital Converter for Determining Root Mean Square Value of the Voltage in the Presence of Higher Harmonics in the Input Signal. – PP. 483–487.
Analog-digital converters are widely used to convert voltage to digital code in various electronic systems. Parallel ADCs are distinguished by their speed, since the parallel circuit

allows all comparators to conduct simultaneously. If the input signal contains higher harmonics, then its shape is distorted relative to the ideal sinusoidal shape, and for the correct voltage calculation, you need to take into account the ADC capacity and its reference voltage.
Key words: higher harmonics, root mean square value of the voltage, analog-digital converter.

Katkova T., Sedyshev E. Microwave Generator on a Ring Elliptic Resonator in a Symmetric Strip Version. – PP. 488–492.
The paper proposes a design of a microwave generator based on an elliptical ring resonator. Computer simulation of the device was carried out using the RFSimm99 program. The geometric dimensions of the device have been calculated. A model of the generator on the micro-strip line has been created.
Key words: microwave generator, active two-pole, resonator, spectrogram.

Konovalova E., Motrenko V., Sedyshev E. Microwave Generator on an Active Two-Pole Device in a Cylindrical Resonator. – PP. 493–497.
Creation of high-stable generators is an actual problem in the field of microwave frequencies. The subject of the study is the generator on the active two-pole device in the cylindrical resonator. In this work the calculation was made of resonant frequencies for three types of electromagnetic vibrations of the cylindrical resonator, depending on its geometric dimensions and filling. Created an experimental stand of the generator, by means of which the presence of generation at the calculated frequencies was checked, the results obtained during the experiment were presented, and the results were compared with the calculations.
Key words: microwave, generator, cylindrical resonator.

Kuznetsova T., Urvantseva N., Urvantsev V. Experimental Verification of Steiner's Theorem using a Torsional Pendulum. – PP. 498–504.
Nothing can replace the student's work with real devices, these are his first steps in research. However, faced with the remote mode of work, everyone began to pay more attention to virtual work. Obviously, the lack of "manual work" must be compensated for by increasing attention to theory and, in particular, to the processing of measurement results. The presented article is devoted to the formulation of a virtual work on the verification of Steiner's theorem.
Key words: laboratory practice, fluctuations, measurement error, least squares method.

Landa A., Larkov E. Experimental Study of Distortion and Noise Suppression by Means of a Double Feedback. – PP. 504–509.
A new method of linearization of a nonlinear amplifier by double feedback is experimentally investigated. Linearization is achieved by a combination of two feedback loops (negative feedback loop and positive feedback loop), in which an auxiliary amplifier is included. For the study, an additional source of interference was included in the circuit (at the output of the main amplifier) which allowed us to conduct a study of distortion suppression on simple equipmen.
Key words: experimental study, Linearization of a nonlinear microwave amplifier, double feedback, suppression of intermodulation distortion.

Landa A., Mugu L. Tunable Frequency-Separation Device on a Ferrospinel Substrate. – PP. 509–512.
The possibility of creating a tunable filter on a ferrospinel was investigated. In microwave electronics, there is a need for tunable filters, and the creation of filters on a ferrite substrate, controlled by a magnetic field, could help solve this problem. In this paper, we investigate the possibility of creating a tunable microstrip filter with three resonators on a ferrospinel substrate.
Key words: microwave, resonator, microwave filters, ferrite substrate, ferrospinel.

Leontyev A., Sedishev E. Synthesis of a Microwave Adder with Energy Input/Output in Different Layers of the Microwave Circuit. – PP. 513–518.
The work is devoted to the design of three-dimensional microwave integrated circuits; the design and layout of a power division device built on strip lines are considered. The interfaces of the proposed adder are located in different layers of three-dimensional microwave integrated circuit. The individual adder nodes and the device as a whole are synthesized. An experiment is conducted, and the features of the functioning of the layouts in the lower part of the microwave range are described. Conclusions are drawn about the efficiency of the power division device under study.
Key words: SHF, power divider, Adder, Symmetrical strip line, strip line, attenuation, wave resistance, double strip line, triple strip line, invert strip line.

Mezhevova M., Filin V. Modeling and Analyzing the Frequency Response of Switch HF Power Amplifiers – PP. 518–522.
The paper describes a technique for computer modeling of the frequency characteristics of switch (nonlinear) HF power amplifiers operating in the class E mode. The technique takes into account the spectra of real steady-state processes, that arise when a harmonic disturbance is imposed on a periodic control action. The calculation results are presented and analyzed.
Key words: high-frequency switch amplifiers, method of equivalent frequency characteristics.

Mustagulova B., Sagyndikova A. Diagnostics of Technical State of Heat Power Objects Based on Information Systems. – PP. 522–528.
The state of heat and power equipment of the Republic of Kazakhstan is presented. The necessity of creating a modern system that will work with the use of retrospective data on the basis of distributed computing infrastructures is shown. Modern information systems of heat and power diagnostics are analyzed, criteria for monitoring the state of heat and power equipment according to its condition are proposed, issues of energy saving and efficient use of energy carriers are the main problem of national security of the Republic of Kazakhstan. The heat and power complex is the basis of the energy sector, the analysis of existing information systems (IS) of heat and power diagnostics and the development of criteria for the further development, implementation and maintenance of IS monitoring and analysis of the modes of operation of heat and power facilities, taking into account their current technical condition. In this regard, the relevance of creating an information system for diagnosing and monitoring the state of heat engineering equipment is beyond doubt.
Key words: heat and power engineering, boiler house, information system, diagnostics, monitoring, distributed computing infrastructure.

Nikitin Yu. Main Regulated Parameters of Voltage Controlled Oscillators. – PP. 529–533.
The main standardized parameters of high-frequency oscillators used in modern frequency synthesizers are considered. These parameters allow you to get a complete picture of the quality of the generated vibrations and the effect of destabilizing influences on them.
Key words: frequency synthesis, pulse-phase-locked loop (PLL), voltage controlled oscillators, spurious spectral components, detector, logarithmic detector, positive feedback, negative feedback.

Nikitin Yu., Sinichkin A. Calculation of a Nanosecond Range Delay Control Device on Bipolar Transistors for a Modified State Machine. – PP. 534–537.
The report is devoted to the selection of elements, calculation and circuit simulation of a controlled delay device (CDD) of the nanosecond range. The obtained result is analyzed to reduce the influence of parasitic capacitances and minimize the nonlinearity of the digital control code conversion in the time interval. Schematic modeling was performed in the Micro-cap software package. To supply an overflow signal to the CDD, a modified finite automaton model is used, built on the basis of a frequency divider with a fractional-variable division factor and an accumulating adder.
Key words: controlled delay device, state machine, accumulator, variable fraction divider, microcap.

Nikitin Yu., Tsygankov G. Simulation of the IFAP Multipliering Ring with NON-Linearities. – PP. 538–542.
The model of a frequency-multiplying pulse-phase-locked loop (PLL) in a MicroCap12 environment is considered. The custom model of a tunable generator with a characteristic specified by a custom table-valued function is using. In the model of the applied phase detector based on two phase-frequency detectors with a charge pumping circuit. The fractional-N divider is implemented on the principle of a delta-sigma modulator. The operation of the ring in the dynamic (when switching the division ratios) mode, as well as the range of the output oscillation in the steady-state (stationary) mode, are considered.
Key words: PLL, spectral components, heterodyne, DFD, PFD, automatic frequency control.

Nikitin Yu., Tsygankov G. Phase Detector Simulation Based on two PFD. – PP. 542–547.
The model of phase detector is investigated in the Microcap 12 environment. The proposed model has a single linear section of the transfer characteristic (without periodicity), which makes it possible to change the pulse-phase-locked loop's frequency in bigger range, while retaining the small role of the nonlinearity zone, as in the original frequency-phase detectors with charge pumping circuit. The characteristics (static transfer characteristic, the value of the nonlinearity zone) of the phase detector pulses in a wide and narrow range of phase delays are considered. A comparative analysis of the use of various phase detectors (phase detector based on an RS flip-flop, frequency-phase detector with a charge pumping circuit) in a pulse-phase-locked loop is performed.
Key words: PLL, frequency spectrum, phase detector, automatic frequency control.

Polyakova A., Sedyshev E. Topology Scaling as a Synthesis Method Microwave Bandpass Filters. – PP. 547–552.
In this paper the problems of microwave filters synthesis are considered. By scaling the geometry of bandpass strip filter on coupled resonators, which is selected as a prototype, scale models of the device are created. As a result of the experiment, it becomes obvious that such devices, the characteristics of which repeated the original one in different frequency regions, are, in fact, new microwave filters with their own technical characteristics.
The created filters are investigated for the central frequency shift and change of the passband width. Various bandpass filter designs were analyzed and the most appropriate scaling techniques were selected.
Key words: synthesis, layout, microwave bandpass filter, strip filter, loop filter, filter with U-shaped resonators, center frequency.

Sedyshev E., Rumyanceva A. Precision Synthesis of Constructive the Inductances of Microwave Integrated Circuits. – PP. 552–557.
The paper analyzes the mathematical apparatus for the synthesis of inductors for microwave integrated circuits. Various methods of synthesis of circular spiral inductors and algorithms for their calculation are considered. The influence of parasitic parameters on the inductance rating is investigated. A comparison of the methods with each other, as well as a comparison of the calculation result with the experiment result is made. The experiment was carried out using various methods for assessing reactivity.
Key words: integrated circuits, microwave frequencies, flat circular spiral inductors, parasitic parameters, quasi-dynamic approximation.

Sedyshev E., Sokovykh R. Ring Elliptical Resonator as an Emitter. – PP. 558–562.
The paper considers the possibility of using an elliptical ring resonator as an emitter with elliptical polarization. In the process of work models of emitters were created, which were powered by a microstrip line. Experiments were carried out and the results were evaluated.
Key words: ring resonator, emitter, elliptical polarization.

Sergeev V. Estimation of the Effect of Losses in LC Filter Elements on the Attenuation Characteristic. – PP. 563–567.
It is shown that for classical reactive low-pass filters with consistent loads, the maximum (in the working domain) attenuation increment due to losses in the elements corresponds to the boundary frequency of the passband and is estimated in terms of the maximum total reactive energy. Simple relations are given to estimate the effect of losses on the change in the unevenness of attenuation in the filter bandwidth.
Key words: reactive filter, the effect of the losses, energy function.

Surkov E., Filin V. Development of a Computer Model and Study of a Microwave Transistor Amplifier Based on a Doherty Circuit. – PP. 568–572.
Described the mechanism of the Doherty power amplifier. A model of this amplifier was created in Fastmean software with the use of piecewise linear substitution scheme of powerful GaN-transistors. The model was designed to amplify a modulated signal with a center frequency of

500 MHz. Power and efficiency values of the amplifier was obtained and compared with values of class AB and C amplifiers.

Key words: power amplifier, Doherty, Fastmean, microwave transistor amplifier, class AB amplifier, class C amplifier.

СВЕДЕНИЯ ОБ АВТОРАХ

АВНИГИНА Александра Викторовна — студент группы ИСТ-931м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aavnigina@mail.ru

АВРАМЕНКО Владимир Семенович — кандидат технических наук, доцент, профессор кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, vsavr@yandex.ru

АДУЕВСКИЙ Александр Михайлович — студент группы ИСТ-951м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Sashabommm341@gmail.com

АКИМОВ Сергей Викторович — кандидат технических наук, доцент кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akimov-sv@yandex.ru

АНДРИАНОВА Екатерина Евгеньевна — старший преподаватель кафедры безопасности информационных систем Санкт-Петербургского университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yekaterina_and@mail.ru

АНИКИЕВА Анастасия Валерьевна — студентка группы ИСТ-031м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nastya97397@gmail.com

АНТОНОВ Валерий Валентинович — старший преподаватель кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, antonler@rambler.ru

АРХИПОВ Михаил Андреевич — сотрудник Академии ФСО России, mdo@academ.msk.rsnet.ru

АРХИПОВА Мария Максимовна — студентка группы ИСТ-931м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, m.m.arkhipova@yandex.ru

АХМЕТШИНА Милена Энверовна — студентка группы ИКТБ-07м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akhmet-mil@mail.ru

БАБАЕВА Алла Васильевна — студентка кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, beljaeva-a@list.ru

БАРАНОВ Игорь Юрьевич — кандидат технических наук, доцент, сотрудник Академии ФСО России, i_baranov@rambler.ru

БАШКИРЦЕВ Андрей Сергеевич — кандидат технических наук, начальник военно-научного комитета Главного управления Связи Вооруженных Сил Российской Федерации, ab098@yandex.ru

БАЯГАНТАЕВА Екатерина Васильевна — студентка группы ИСТ-032м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, e.bayagantaeva@mail.ru

БЕЛОВ Станислав Михайлович — магистр кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, madl@inbox.ru

БЕЛОУС Константин Владимирович — кандидат технических наук, доцент кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kostos2@yandex.ru

БОНДАРЕНКО Игорь Борисович — кандидат технических наук, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, igorbnd@gmail.com

БОЧАРОВ Евгений Иванович — кандидат технических наук, доцент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bocharov.ekp@gmail.com

БРАНИЦКИЙ Александр Александрович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexander.branitskiy@gmail.com

БРУСИН Ефим Александрович — кандидат технических наук, доцент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; начальник научно-технического отдела, Научно-исследовательский институт радио Санкт-Петербургский филиал «Ленинградское отделение научно-исследовательского института радио», yefim@loniir.ru

БУНЯКИНА Екатерина Витальевна — старший преподаватель кафедры информационных технологий Военно-морского политехнического института ВУНЦ ВМФ «Военно-морская академия», school5572007@yandex.ru

ВАГАНОВ Александр Валерьевич — старший преподаватель кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sut-ispiu@mail.ru

ВАРЛАМОВ Михаил Игоревич — сотрудник Академии ФСО России, tsibul@mail.ru

ВАСИЛЬЧЕНКО Валентина Дмитриевна — студентка кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vas.valenti@yandex.ru

ВЕЛИКОБОРЕЦ Глеб Сергеевич — студент 3 курса факультета радиотехнологий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, glebsrojects@mail.ru

ВЕЛЮГО Артем Михайлович — аспирант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, velugo.a@gmail.com

ВЕРХОВА Галина Викторовна — доктор технических наук, профессор, заведующая кафедрой интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, galina500@inbox.ru

ВИШНЕВСКИЙ Андрей Сергеевич — сотрудник Академии ФСО России, mdo@academ.msk.rsnet.ru

ВЛАДЫКИН Максим Валерьевич — студент группы ИСТ-931м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladykinmv@gmail.com

ВОЛОШИНОВ Денис Вячеславович — доктор технических наук, заведующий кафедрой информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, denis.voloshinov@yandex.ru

ВОЛЫНКИН Павел Александрович — кандидат технических наук, доцент кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pavelas@mail.ru

ВОСТРЫХ Алексей Владимирович — аспирант Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.vostrykh@list.ru

ГАЛЬЧЕНКО Максим Иванович — старший преподаватель кафедры электроэнергетики и электрооборудования Санкт-Петербургского государственного аграрного университета, maxim.galchenko@gmail.com

ГЕНЧЕВА Алёна Валерьевна — студентка группы ИСТ-713 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alyona_gen@mail.ru

ГЛУХОВ Николай Иванович — старший преподаватель, заведующий лабораторией кафедры электроники и схемотехники Санкт-Петербургского университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, glukhov_nikolay@mail.ru

ГОРОХОВ Александр Владимирович — оператор роты (научной) Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, sanya.gorokhov.97@mail.ru

ГОРШЕНИНА Александра Никитична — студентка группы ИСТ-931м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gorshenina@bonch.dev

ГРИШИН Никита Александрович — студент группы ИКТЗ-01М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, smerh-8@yandex.ru

ГРОМОВ Владислав Витальевич — кандидат технических наук, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gromov_vladislav@hotmail.com

ГУБИН Александр Николаевич — кандидат технических наук, доцент, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gan50_60@mail.ru

ГУНИНА Елена Викторовна — кандидат педагогических наук, доцент, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, e.v.gunina@yandex.ru

ГУЩИНСКИЙ Александр Геннадьевич — кандидат технических наук, ведущий инженер Учебного комплекса ПАО «Россети Ленэнерго»

ДАВЛЕТШИНА Элеонора Ринатовна — магистрант группы ИСТ-941м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, eleonora.davletshina@mail.ru

ДАГАЕВ Александр Владимирович — кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, adagaev@list.ru

ЕЛГИН Павел Игоревич — ведущий инженер научно-технического отдела Научно-исследовательского института радио Санкт-Петербургский филиал «Ленинградское отделение научно-исследовательского института радио», elgin.pavel@gmail.com

ЕРЕМЕНКО Александр Иванович — кандидат технических наук, доцент, сотрудник Академии ФСО России, EAI6464@mail.ru

ЖАРАНОВА Анастасия Олеговна — студентка группы ИСТ-911м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zharanovaan@gmail.com

ИВАНОВ Алексей Сергеевич — студент магистратуры группы ИСТ-941м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aleks_1503@mail.ru

ИВАНОВ Сергей Александрович — кандидат технических наук, докторант Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, sa-ivanov@inbox.ru

ИВАНОВА Светлана Владимировна — студент группы ИСТ-931м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivanova2530@bk.ru

ИЗРАИЛОВ Константин Евгеньевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; старший научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, Konstantin.Izrailov@mail.ru

ИЛЬИНА Ольга Борисовна — кандидат географических наук, доцент, старший преподаватель кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, nastik94@yandex.ru

КАЗАКЕВИЧ Елена Владимировна — кандидат технических наук, доцент кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I, kev-pgups@yandex.ru

КАТКОВА Татьяна Олеговна — студент магистратуры группы ФП-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича tatyana.katkova.98@mail.ru

КОВАЛЕНКО Леонид Александрович — студент группы ИКПИ-85 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, canyone2015@yandex.ru

КОЗИН Сергей Сергеевич — сотрудник Академии ФСО России, mdo@academ.msk.rsnet.ru

КОКОРЕВ Антон Владимирович — кандидат физико-математических наук, сотрудник Академии ФСО России, interline57@mail.ru

КОЛЕСОВ Даниил Сергеевич — студент магистратуры группы ИСТ-941м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, KolesovD98@gmail.com

КОЛОСКОВ Никита Андреевич — студент группы ИСТ-032м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nikita.koloskooov@gmail.com

КОЛЬЦОВ Павел Олегович — студент магистратуры группы ИСТ-032м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zemtirstudio@gmail.com

КОНОВАЛОВА Елизавета Александровна — студентка магистратуры группы ФП-91м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, konowalowa.elizaweta@yandex.ru

КОНОНЮК Ольга Алексеевна — студентка группы ИСТ-941м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hola.aloha@outlook.com

КОРШУНОВ Михаил Владимирович — ведущий инженер научно-технического отдела Научно-исследовательского института радио Санкт-Петербургский филиал «Ленинградское отделение научно-исследовательского института радио», korshunov@loniir.ru

КОСОВ Никита Алексеевич — ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. М. А. Бонч-Бруевича, kosov.n.a@mail.ru

КОСОЛАПОВ Владислав Сергеевич — адъюнкт Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, kvs_mil@mail.ru

КРАВЧЕНКО Анна-Мария Михайловна — студентка группы ИСТ-931м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kravcenkoamm@gmail.com

КРИВОНОСОВА Наталья Викторовна — преподаватель Санкт-Петербургского колледжа телекоммуникаций им. Э. Т. Кренкеля, nvkrivonosowa@mail.ru

КРЮКОВА Елена Сергеевна — адъюнкт (аспирант) кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, e.kkrukovaa69@yandex.ru

КУЗНЕЦОВА Татьяна Евгеньевна — кандидат физико-математических наук, доцент, пенсионер, tanuhakuznetsova@gmail.com

КУПЦОВ Алексей Викторович — студент магистратуры группы ИСТ-941м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, i.leha98@mail.ru

КУПЧИНЕНКО Ольга Павловна — преподаватель кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, k-olga102@yandex.ru

Кучеревский Кирилл Владимирович — студент группы ИСТ-951м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, x1ebylliek2k@gmail.com

ЛАНДА Александр Эдуардович — кандидат технических наук, доцент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, landa.alexandr@mail.ru

ЛАРЬКОВ Евгений Юрьевич — студент магистратуры группы ФП-91м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, jlarkov@gmail.com

ЛЕОНТЬЕВ Александр Сергеевич — студент магистратуры Санкт-Петербургского государственного университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, leontev.aleksandr.88@mail.ru

ЛЕПЕШКИН Олег Михайлович — доктор технических наук, доцент, доцент кафедры безопасности инфокоммуникационных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, lepechkin1@yandex.ru

ЛЕПИХИН Кирилл Алексеевич — студент магистратуры группы ФП-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kirilllepi@mail.ru

ЛИПАНОВА Ирина Александровна — кандидат технических наук, доцент кафедры безопасности информационных систем Санкт-Петербургского университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lipanova@mail.ru

ЛИПАТНИКОВ Валерий Алексеевич — доктор технических наук, профессор, старший научный сотрудник Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, lipatnikovanl@mail.ru

ЛИТВИНОВ Владислав Леонидович — кандидат технических наук, доцент, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vlad.litvinov61@gmail.com

МАЗЕПИН Павел Сергеевич — студент группы ИКТЗ-01М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, flinkaforever@gmail.com

МАКАРОВ Леонид Михайлович — кандидат технических наук, доцент, доцент кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, biopet@mail.ru

МАЛИКОВ Альберт Валерьянович — заместитель начальника отдела Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, mkv.vas@yandex.ru

МАНКАЕВ Расул Мурат-Алиевич — студент группы ИКТБ-07м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 24rasul1999@mail.ru

МАНУКОВ Кирилл Олегович — слушатель Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, oleg-26stav@mail.ru

МАРДАНОВ Ринат Ильдарович — студент группы ИКТБ-08м кафедры защищенных систем связи института магистратуры Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gyxepm@gmail.com

МАРКИН Дмитрий Олегович — кандидат технических наук, сотрудник Академии ФСО России, mdo@academ.msk.rsnet.ru

МАРТЫНОВ Денис Игоревич — студент группы ИСТ-911м Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, madengic@gmail.com

МАСЛАКОВ Михаил Леонидович — кандидат технических наук, научный сотрудник АО «Российский институт мощного радиостроения», maslakovml@gmail.com

МАХОРТОВ Сергей Валерьевич — студент магистратуры группы ИСТ-032м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, PartOfCat@yandex.ru

МЕЖЕВОВА Мария Александровна — аспирантка кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, m.kondrashova2010@yandex.ru

МЕТЕЛЬКОВ Александр Николаевич — кандидат юридических наук, доцент кафедры прикладной математики и информационных технологий Санкт-Петербургского университета МЧС России, metelkov5178@mail.ru

МИНАЧЁВ Владислав Маратович — сотрудник Академии ФСО России, mdo@academ.msk.rsnet.ru

МИХАЙЛИЧЕНКО Антон Валерьевич — соискатель Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, 23esn2008@rambler.ru

МИХАЙЛИЧЕНКО Николай Валерьевич — кандидат технических наук, преподаватель кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, 23esn2008@rambler.ru

МИХАЛЬ Георгий Андреевич — студент группы ИСТ-712 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vat-reg@yandex.ru

МОГУШ Людмила Станиславовна — студентка группы ИСТ-912м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gsmorodin@gmail.com

МОТРЕНКО Валентин Иванович — студент магистратуры группы ФП-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, motrenko-mw@yandex.ru

МУГУ Лилия Рашидовна — студентка группы ФП-91м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, liliamugu@gmail.com

МУСАЕВА Татьяна Вагиф кызы — кандидат технических наук, доцент, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, neli_6868@mail.ru

МУСТАГУЛОВА Бопа Жанабаевна — Алматинский университет энергетики и связи имени Гумарбека Даукеева, b.mustagulova@aues.kz

НИКИТИН Юрий Александрович — кандидат технических наук, старший научный сотрудник, доцент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yuriyan@list.ru

НИКИФОРОВА Екатерина Алексеевна — сотрудник Академии ФСО России, mdo@academ.msk.rsnet.ru

НОВИКОВ Егор Анатольевич — студент группы ИСТ-711 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, egoredmc@gmail.com

ОДНОКУРЦЕВ Кирилл Андреевич — старший оператор роты (научной) Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, kirillodn@mail.ru

ОЛИМПИЕВ Алексей Александрович — кандидат технических наук, доцент кафедры интеллектуальные системы автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aao_82@mail.ru

ОРЛОВ Дмитрий Андреевич — студент группы ИКТБ-08м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, orlovsut62@gmail.com

ОСТРОУМОВ Максим Александрович — начальник отделения кафедры безопасности инфокоммуникационных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, coj1991@mail.ru

ОСТРОУМОВ Олег Александрович — кандидат технических наук, докторант кафедры безопасности инфокоммуникационных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, oleg-26stav@mail.ru

ПАВЛОВИЧ Артур Александрович — кандидат технических наук, доцент кафедры автоматизации предприятий связи Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, fathertal@mail.ru

ПАНОВ Артем Александрович — сотрудник Академии ФСО России, i_baranov@rambler.ru

ПАРАЩУК Игорь Борисович — доктор технических наук, профессор, Заслуженный изобретатель РФ, профессор кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, shchuk@rambler.ru

ПЕТРОВ Георгий Валентинович — сотрудник Академии ФСО России, petrovkazanksvu@mail.ru

ПИЛИКИНА Елена Анатольевна — старший преподаватель кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, helenarh@yandex.ru

ПЛЕТНЕВ Ярослав Андреевич — аспирант кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, pletnevyaroslav@gmail.com

ПОГАДАЕВА Ольга Павловна — студентка магистратуры группы ИСТ-031м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, olgakoelliker14@gmail.com

ПОДОЛЬСКАЯ Мария Олеговна — студентка магистратуры группы ФП-91м Санкт-Петербургского государственного университета, masha.bas@yandex.ru

ПОКУСОВ Виктор Владимирович — председатель Казахстанской Ассоциации Информационной Безопасности, v@victor.kz

ПОЛЯКОВА Анастасия Валерьевна — студентка магистратуры группы ФП-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nastyapool@mail.ru

ПОПОВА Валерия Олеговна — аспирантка факультета безопасности информационных технологий университета ИТМО, lerapopova236@gmail.com

ПРИСЯЖНЮК Андрей Сергеевич — кандидат технических наук, исполнительный директор ЗАО «Институт телекоммуникаций», pas@itain.ru

ПРОКОФЬЕВ Павел Александрович — аспирант кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sometech@mail.ru

ПТИЦЫНА Лариса Константиновна — доктор технических наук, профессор, заведующая кафедрой информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ptitsina_lk@inbox.ru

ПУЗАНОВ Иван Сергеевич — студент магистратуры группы ИСТ-031м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivan.puzanov140@icloud.com

РАДНАЕВА Ирина Юрьевна — студентка кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, i.y.radnaeva@gmail.com

РОЖДЕСТВЕНСКИЙ Дмитрий Борисович — студент группы ИСТ-031м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitriifoxqq2@gmail.com

РУЙГО Даниил Иванович — студент группы ИСТ-012м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, smolldru@gmail.com

РУМЯНЦЕВА Анастасия Максимовна — студентка магистратуры группы ФП-01М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 1228amrumanceva@mail.ru

РЫКОВ Даниил Алексеевич — сотрудник Академии ФСО России, mdo@academ.msk.rsnet.ru

САВИН Максим Юрьевич — студент группы ИСТ-941м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 78obahir@gmail.com

САГЫНДИКОВА Айгул Журсиновна — Алматинский университет энергетики и связи имени Гумарбека Даукеева, a.sagyndikova@aues.kz

САЛМАН Васан Давуд — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, wasan.salman@mail.ru

СЕДЫШЕВ Эрнест Юрьевич — кандидат технических наук, доцент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, laboratoria-mw@yandex.ru

СЕРГЕЕВ Валерий Варламович — доктор технических наук, профессор кафедры теории электрических цепей и связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, vsergv43@mail.ru

СЕРГИЕНКО София Сергеевна — студентка группы ИСТ-031м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ssssofisss@gmail.com

СЕРЕГИН Сергей Сергеевич — студент группы ИСТ-941м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, serezha.seregin@gmail.com

СИНИЧКИН Александр Александрович — Студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alrksandr.sin@gmail.com

СИНЮК Александр Демьянович — доктор технических наук, доцент, профессор кафедры общепрофессиональных дисциплин Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, eentrop@rambler.ru.

СКОРОБОГАТОВ Иван Иванович — сотрудник Академии ФСО России, i_baranov@rambler.ru

СКОРОБОГАТОВ Кирилл Денисович — студент группы ИСТ-032м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kirill9806@gmail.com

СКОРОПАД Александр Витальевич — ведущий инженер-электроник НИЛ №4131, НИО №413, НТЦ №41 Санкт-Петербургского филиала «Ленинградское отделение научно-исследовательского института радио», sav01236@yandex.ru

СЛЕСАРЧИК Константин Федорович — сотрудник Академии ФСО России, interline57@mail.ru

СМИРНОВ Иван Юрьевич — адъюнкт Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, sensemile.nic@mail.ru

СМОРОДИН Геннадий Николаевич — кандидат технических наук, старший преподаватель кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gsmorodin@gmail.com

СОКОВЫХ Регина Игоревна — студентка магистратуры группы ФП-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sokovih_regina@mail.ru

СОЛОВЬЕВ Денис Викторович — кандидат технических наук, доцент кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 9218964588@mail.ru

СУРКОВ Эдвард — студент магистратуры группы ФП-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, edvard11@mail.ru

ТАРАСОВ Александр Алексеевич — адъюнкт кафедры общепрофессиональных дисциплин Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, taras4912@mail.ru

ТАРАСОВ Владимир Анатольевич — старший преподаватель кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vat-liquidator@bk.ru

ТАТАРНИКОВА Ирина Михайловна — аспирант кафедры Безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, itatarnikova@list.ru

ТЕРЕЩЕНКО Николай Евгеньевич — студент группы К-580 Санкт-Петербургского колледжа телекоммуникаций им. Э. Т. Кренкеля, moctt123@gmail.com

ТИТОВ Сергей Владимирович — слушатель Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, oleg-26stav@mail.ru

ТРЕПАЛИН Павел Викторович — старший оператор роты (научной) Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, trepalin98@mail.ru

УКРАИНЕЦ Юлия Олеговна — студентка группы ИСТ-931м Санкт-Петербургского государственного университета телекоммуникаций им. М. А. Бонч-Бруевича, ramjul@mail.ru

УРВАНЦЕВ Владимир Георгиевич — кандидат технических наук, пенсионер, vladimir-urvancev@rambler.ru

УРВАНЦЕВА Наталия Львовна — кандидат технических наук, доцент кафедры физики Санкт- Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, N.Urv@yandex.ru

УШАКОВ Игорь Александрович — кандидат технических наук, старший преподаватель Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ushakovia@gmail.com

ФАДЕЕВ Вадим Владиславович — сотрудник Академии ФСО России, tsibul@mail.ru

ФЕДОРОВ Павел Николаевич — старший научный сотрудник научно-исследовательского центра Военной орденов Жукова и Ленина Краснознаменной академии связи им. Маршала Советского Союза С. М. Буденного, sensemile.nic@mail.ru

ФЁДОРОВ Никита Сергеевич — студент магистратуры группы ИСТ-941м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fyodorov.ns@gmail.com

ФЕДОРОВА Алина Владимировна — кандидат экономических наук, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, asp@spbgut.ru

ФИЛИН Владимир Алексеевич — доктор технических наук, профессор, заведующий кафедрой электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, filin_vladimir@mail.ru

ФИЛИППОВ Феликс Васильевич — кандидат технических наук, старший научный сотрудник, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 9000096@mail.ru

ФРОЛОВА Кристина Александровна — аспирант кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, frolkris988@gmail.com

ХОРОШЕНКО Виктория Сергеевна — аспирант кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, xoroshenko.v@mail.ru

ЦИБУЛЯ Алексей Николаевич — кандидат технических наук, доцент, сотрудник Академии ФСО России, tsibul@mail.ru

ЦЫГАНКОВ Григорий Антонович — студент группы ФП-91м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, uhbifka1@gmail.com

ЧЕРНОБРОВКИН Евгений Михайлович — студент группы ИСТ-712 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vat-reg@yandex.ru

ЧЕРНОМЫРДИН Владимир Викторович — студент группы ИСТ-931М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vov.cher@mail.ru

ЧЕЧУЛИН Андрей Алексеевич — кандидат технических наук, доцент, ведущий научный сотрудник Лаборатории проблем компьютерной безопасности СПИИРАН Санкт-Петербургского федерального исследовательского центра Российской академии наук, andreych@bk.ru

ЧМЕЛЁВ Михаил Эдуардович — студент группы ИКВТ-82 Санкт-Петербургского государственного университета, chmelev.mikhail@gmail.com

ШАБАНОВ Александр Павлович — магистрант кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shabanov.ap@shpg.spb.ru

ШВЕДОВ Сергей Николаевич — кандидат технических наук, сотрудник Академии ФСО России, s_shvedov112@mail.ru

ШЕСТАКОВ Александр Викторович — доктор технических наук, старший научный сотрудник, профессор кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexandr.shestakov01@yandex.ru

ШИЯН Андрей Анатольевич — кандидат педагогических наук, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 1001digit@gmail.com

ЩУКИН Артем Владимирович — сотрудник Академии ФСО России, mdo@academ.msk.rsnet.ru

ЮРОВА Валентина Александровна — кандидат физико-математических наук, доцент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, va-yurova@mail.ru

ЯКОВЛЕВ Виктор Алексеевич — доктор технических наук, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, viyak@bk.ru

ЯРОШЕНКО Александр Юрьевич — начальник отдела организации защиты информации Департамента информационных технологий и связи МЧС России, alexagz@mail.ru

АВТОРСКИЙ УКАЗАТЕЛЬ

СПбГУТ)))